PROCEDURA ZARZĄDZANIA CYBERBEZPIECZEŃSTWEM

Przedszkole Nr 4

"Pod zielonym listkiem"

ul. Z. Padlewskiego 3,

09-100 Płońsk

……..……..……

(nazwa podmiotu)

mgr Barbara Kostrzewa

……..

(imię i nazwisko osoby reprezentującej podmiot)

Dyrektor

……..

(pełniona funkcja / zajmowane stanowisko)

W codziennej działalności Placówka funkcjonuje w środowisku cyfrowym, korzystając z wielu systemów teleinformatycznych oraz aplikacji, co sprawia, że zagadnienia związane z cyberbezpieczeństwem mają kluczowe znaczenie dla prawidłowego i bezpiecznego realizowania zadań.

Dynamiczny rozwój technologii oraz powszechny dostęp do zasobów Internetu powodują wzrost liczby zagrożeń, wynikających zarówno z niewystarczających zabezpieczeń technicznych, jak i z niewłaściwego korzystania z systemów informatycznych przez użytkowników.

Podmioty świadczące usługi informatyczne i teleinformatyczne zobowiązane są do zapewnienia ciągłości działania systemów, a także do ochrony poufności, integralności i dostępności przetwarzanych informacji.

Mając na uwadze rosnące ryzyko wystąpienia incydentów cyberbezpieczeństwa oraz konieczność podejmowania działań prewencyjnych, niniejszy dokument został opracowany w celu wsparcia Administratorów Danych w podnoszeniu poziomu bezpieczeństwa informacji poprzez dostarczenie wiedzy oraz praktycznych rozwiązań organizacyjnych i technicznych, służących ochronie Podmiotu przed potencjalnymi cyberzagrożeniami.

Spis treści

I. Wstęp

Niniejszy dokument stanowi wewnętrzną regulację obowiązującą w Placówce, określającą zasady zapewnienia cyberbezpieczeństwa oraz zarządzania ryzykiem związanym z funkcjonowaniem systemów informatycznych. Dokument opiera się na podejściu proaktywnym, uwzględniającym zasadę ciągłego doskonalenia, w szczególności poprzez identyfikację zagrożeń, analizę ryzyka oraz wdrażanie adekwatnych środków technicznych i organizacyjnych w odniesieniu do wykorzystywanych systemów i aplikacji informatycznych.

Adresatami niniejszego dokumentu są osoby fizyczne i prawne uczestniczące w przetwarzaniu informacji, w tym danych osobowych, przy wykorzystaniu systemów teleinformatycznych, aplikacji oraz rozwiązań informatycznych stosowanych w Podmiocie.

Administrator Danych, a w przypadku podmiotów publicznych również kierownik jednostki, zobowiązany jest do podejmowania działań mających na celu zapewnienie odpowiedniego poziomu bezpieczeństwa fizycznego i technicznego, służących ochronie sieci oraz systemów informatycznych przed zagrożeniami, w szczególności wynikającymi z takich zdarzeń jak:

- kradzież lub utrata sprzętu i nośników danych,
- pożar, zalanie lub inne zdarzenia losowe,
- niekorzystne warunki atmosferyczne,
- awarie systemów telekomunikacyjnych,
- przerwy lub zakłócenia w dostawie energii elektrycznej,
- błędy ludzkie,
- awarie systemów i oprogramowania,
- działania złośliwe, w tym cyberataki,
- inne zdarzenia mogące mieć wpływ na poufność, integralność lub dostępność informacji.

Wdrożenie niniejszego dokumentu ma na celu w szczególności:

- zmniejszenie ryzyka operacyjnego poprzez identyfikację słabości w obszarze bezpieczeństwa infrastruktury informatycznej i aplikacji oraz usprawnienie procesów organizacyjnych związanych z ochroną przed zagrożeniami cybernetycznymi,
- potwierdzenie dochowania należytej staranności przez Podmiot w zakresie zapewnienia bezpieczeństwa informacji oraz ochrony danych, w tym danych osobowych,
- podniesienie świadomości i kompetencji pracowników w obszarze cyberbezpieczeństwa.

Dokument zawiera zbiór zasad, procedur i wytycznych opracowanych w celu zapewnienia zgodności działalności Podmiotu z obowiązującymi przepisami prawa, w szczególności:

1. ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U.2024.1077.),
2. rozporządzeniem Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych oraz wymiany informacji w postaci elektronicznej,
3. dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii (NIS2),
4. rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO) – w zakresie, w jakim incydenty cyberbezpieczeństwa mogą skutkować naruszeniem ochrony danych osobowych.

Krajowe podmioty w zakresie nadzoru i kontroli

W krajowym systemie cyberbezpieczeństwa funkcjonują zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), działające na poziomie krajowym, do których zgłaszane są incydenty cyberbezpieczeństwa zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa:

- **CSIRT GOV** – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego, właściwy w szczególności dla podmiotów administracji publicznej;
- **CSIRT MON** – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Ministra Obrony Narodowej;
- **CSIRT NASK** – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy.

Zakres właściwości poszczególnych CSIRT wynika z przepisów ustawy o krajowym systemie cyberbezpieczeństwa.

II. Definicje

Na potrzeby niniejszego dokumentu przyjmuje się następujące definicje:

Cyberbezpieczeństwo – odporność systemów informatycznych na działania naruszające poufność, integralność, dostępność lub autentyczność danych lub usług świadczonych za ich pomocą.

Incydent – zdarzenie, które ma lub może mieć negatywny wpływ na cyberbezpieczeństwo systemów informatycznych.

Incydent krytyczny – incydent powodujący poważne skutki dla bezpieczeństwa państwa, porządku publicznego, zdrowia lub życia ludzi, praw i wolności obywatelskich albo funkcjonowania instytucji publicznych, klasyfikowany przez właściwy CSIRT.

Incydent poważny – incydent, który powoduje lub może powodować istotne zakłócenie ciągłości działania systemów informatycznych lub realizacji zadań Podmiotu i podlega zgłoszeniu do właściwego CSIRT zgodnie z przepisami ustawy o krajowym systemie cyberbezpieczeństwa.

Incydent istotny – incydent mający zauważalny wpływ na funkcjonowanie systemów informatycznych Podmiotu lub realizację jego zadań, niewymagający zgłoszenia do CSIRT, lecz podlegający obsłudze wewnętrznej.

Incydent w podmiocie publicznym – incydent, który powoduje lub może powodować zakłócenie realizacji zadania publicznego.

Obsługa incydentu – zespół działań obejmujących wykrywanie, rejestrowanie, analizę, klasyfikację, podejmowanie działań naprawczych oraz ograniczanie skutków incydentu.

Podatność – cecha systemu informatycznego lub organizacji, która może zostać wykorzystana przez zagrożenie cyberbezpieczeństwa.

Ryzyko – kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego oraz jego skutków.

Szacowanie ryzyka – proces identyfikacji, analizy i oceny ryzyka.

System informatyczny – system teleinformatyczny wraz z przetwarzanymi w nim danymi, wykorzystywany do realizacji zadań Podmiotu.

Zagrożenie cyberbezpieczeństwa – potencjalna przyczyna wystąpienia incydentu.

Zarządzanie incydentem – działania mające na celu obsługę incydentu, usunięcie jego przyczyn oraz zapobieganie jego ponownemu wystąpieniu.

Zarządzanie ryzykiem – skoordynowane działania w zakresie identyfikacji, analizy i ograniczania ryzyka cyberbezpieczeństwa.

III. System cyberbezpieczeństwa

System cyberbezpieczeństwa ma na celu zapewnienie odpowiedniego poziomu bezpieczeństwa systemów informatycznych, w szczególności poprzez zapobieganie incydentom, reagowanie na incydenty oraz ograniczanie ich skutków, w sposób zapewniający ciągłość realizacji zadań Podmiotu.

W ramach krajowego systemu cyberbezpieczeństwa funkcjonują w szczególności:

- podmioty publiczne realizujące zadania publiczne,
- operatorzy usług kluczowych,
- dostawcy usług cyfrowych,
- organy właściwe do spraw cyberbezpieczeństwa,
- zespoły CSIRT,
- Pełnomocnik Rządu do spraw Cyberbezpieczeństwa,
- Kolegium do spraw Cyberbezpieczeństwa.

Zakres obowiązków Podmiotu w ramach systemu cyberbezpieczeństwa jest uzależniony od jego statusu prawnego oraz charakteru realizowanych zadań.

I. Podmioty pełniące funkcję operatora usług kluczowych.

Operatorami usług kluczowych są podmioty, które na podstawie decyzji właściwego organu zostały uznane za świadczące usługi o kluczowym znaczeniu dla funkcjonowania państwa lub gospodarki, w szczególności w sektorach takich jak energia, transport, bankowość, ochrona zdrowia, zaopatrzenie w wodę czy infrastruktura cyfrowa.

Niniejszy dokument **nie przesądza o posiadaniu przez Podmiot statusu operatora usług kluczowych**, o ile status ten nie został formalnie nadany w drodze decyzji administracyjnej.

Obowiązki operatorów usług kluczowych (jeżeli dotyczy)

Do podstawowych obowiązków operatorów usług kluczowych należą w szczególności:

- obsługa incydentów cyberbezpieczeństwa,
- prowadzenie rejestru incydentów,
- klasyfikowanie incydentów zgodnie z obowiązującymi przepisami,
- zgłaszanie incydentów poważnych do właściwego CSIRT w terminach określonych w ustawie,
- współpraca z właściwym CSIRT w trakcie obsługi incydentów,
- usuwanie podatności, które doprowadziły lub mogły doprowadzić do wystąpienia incydentu.

Zgłoszenia incydentów dokonywane są przy wykorzystaniu dostępnych środków komunikacji elektronicznej, zgodnie z obowiązującymi przepisami.

IV. Zgłoszenie incydentu krytycznego lub incydentu poważnego

Zgłoszenie incydentu krytycznego lub incydentu poważnego do właściwego zespołu CSIRT powinno zawierać informacje niezbędne do oceny charakteru i skutków incydentu oraz podjęcia działań koordynacyjnych, w szczególności:

- dane podmiotu zgłaszającego, w tym nazwę, formę organizacyjno-prawną, siedzibę oraz dane kontaktowe;
- imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby dokonującej zgłoszenia;
- imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do udzielania wyjaśnień dotyczących zgłoszonego incydentu;
- opis incydentu oraz jego wpływu na funkcjonowanie Podmiotu, w tym w szczególności:
  a) systemy informatyczne, usługi lub procesy, których dotyczy incydent,
  b) liczbę użytkowników lub zakres odbiorców, na których incydent miał wpływ,
  c) moment wystąpienia incydentu, moment jego wykrycia oraz czas trwania,
  d) obszar lub zakres działania, którego dotyczy incydent,
  e) wpływ incydentu na realizację zadań Podmiotu lub – jeżeli dotyczy – na świadczenie usług przez inne podmioty,
  f) przypuszczalną lub ustaloną przyczynę incydentu, sposób jego przebiegu oraz skutki oddziaływania na systemy informatyczne lub usługi,
  g) informacje umożliwiające właściwemu CSIRT ocenę, czy incydent może mieć charakter transgraniczny lub dotyczyć innych państw członkowskich Unii Europejskiej,
  h) informacje o podjętych lub planowanych działaniach zapobiegawczych,
  i) informacje o podjętych działaniach naprawczych lub ograniczających skutki incydentu,
  j) inne istotne informacje mogące mieć znaczenie dla obsługi incydentu.

Zakres informacji przekazywanych w zgłoszeniu może być uzupełniany w toku obsługi incydentu, w miarę pozyskiwania nowych danych.

V. Obowiązki operatorów usług kluczowych

W przypadku otrzymania przez Podmiot **decyzji administracyjnej właściwego organu** uznającej go za operatora usługi kluczowej, Podmiot realizuje obowiązki wynikające z **ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U.2024.1077)**, w zakresie i terminach określonych w tej ustawie oraz w decyzji organu właściwego.

Niniejszy dokument **nie przesądza o posiadaniu przez Podmiot statusu operatora usług kluczowych**, o ile status ten nie został formalnie nadany w drodze decyzji administracyjnej.

1. Obowiązki podstawowe operatora usług kluczowych

Operator usług kluczowych zobowiązany jest w szczególności do:

- przeprowadzania i aktualizowania analizy ryzyka dla systemów informatycznych wykorzystywanych do świadczenia usług kluczowych,
- wdrażania adekwatnych do oszacowanego ryzyka środków technicznych i organizacyjnych,
- zapewnienia obsługi incydentów cyberbezpieczeństwa,
- prowadzenia rejestru incydentów oraz gromadzenia informacji o zagrożeniach i podatnościach,
- wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z właściwymi zespołami CSIRT oraz organami właściwymi do spraw cyberbezpieczeństwa,
- stosowania środków zapobiegających oraz ograniczających wpływ incydentów na bezpieczeństwo systemów informatycznych,
- prowadzenia działań edukacyjnych i podnoszących świadomość użytkowników w zakresie cyberbezpieczeństwa,
- opracowania i stosowania wymaganej dokumentacji z zakresu cyberbezpieczeństwa,
- zgłaszania incydentów poważnych i krytycznych do właściwego CSIRT w terminach określonych w przepisach prawa,

- usuwania zidentyfikowanych podatności, które doprowadziły lub mogły doprowadzić do wystąpienia incydentu.

2. Audyt bezpieczeństwa

Operator usług kluczowych zobowiązany jest do przeprowadzenia audytu bezpieczeństwa systemów informatycznych, w terminach oraz w zakresie określonym w przepisach ustawy o krajowym systemie cyberbezpieczeństwa oraz w decyzji organu właściwego, a następnie do przekazania sprawozdania z audytu właściwym organom.

VI. Odpowiedzialność i sankcje za naruszenie obowiązków z zakresu cyberbezpieczeństwa

Niewykonanie lub nienależyte wykonanie obowiązków wynikających z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U.2024.1077) może skutkować nałożeniem administracyjnych kar pieniężnych przez właściwy organ, zgodnie z przepisami tej ustawy.

Zakres odpowiedzialności oraz wysokość ewentualnych kar uzależnione są od charakteru naruszenia, statusu podmiotu (w szczególności operatora usługi kluczowej lub dostawcy usługi cyfrowej), stopnia zawinienia oraz skutków naruszenia.

Kary administracyjne mogą być nałożone w szczególności za:

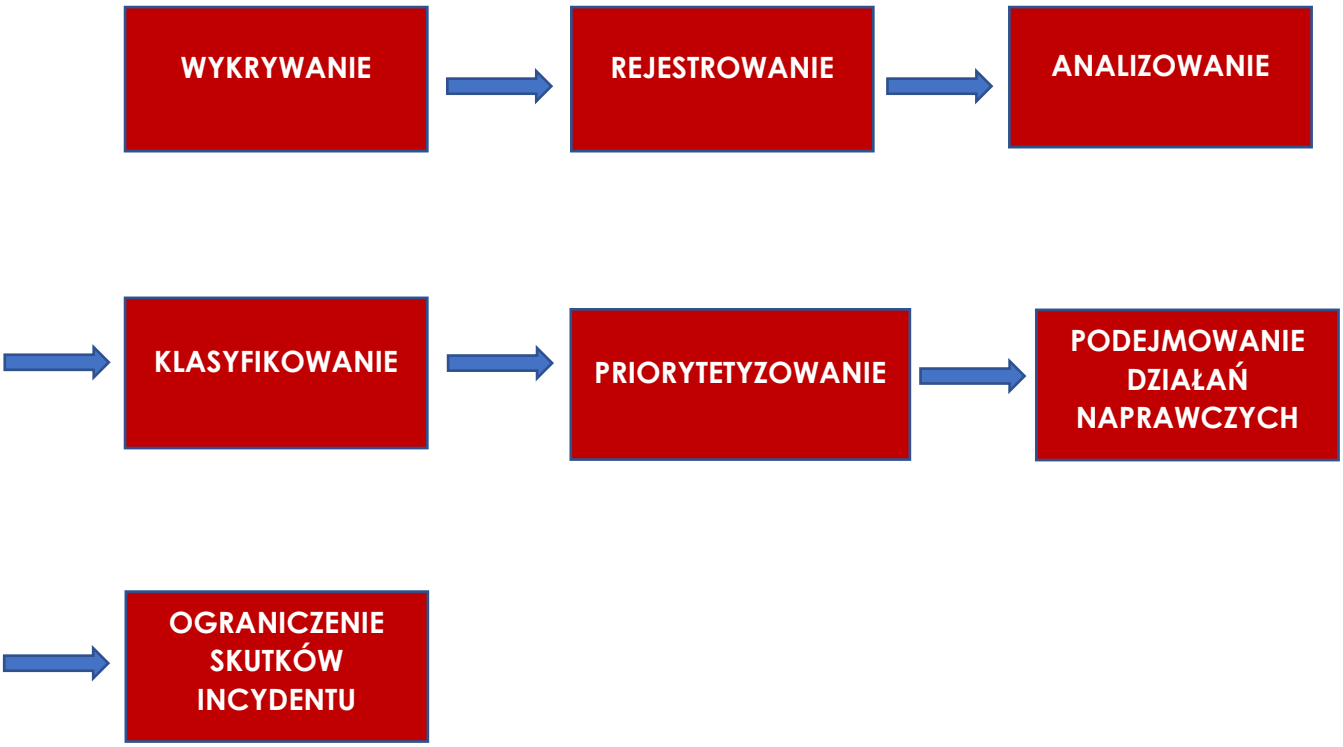
1. brak przeprowadzania lub aktualizacji analizy ryzyka cyberbezpieczeństwa albo brak zarządzania ryzykiem w sytuacji wystąpienia incydentu;
2. niewdrożenie adekwatnych środków technicznych i organizacyjnych służących zapewnieniu bezpieczeństwa systemów informatycznych;
3. niezastosowanie środków zapobiegających oraz ograniczających skutki incydentów, w szczególności w zakresie zapewnienia poufności, integralności, dostępności i autentyczności danych;
4. niewyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa;

5. brak wymaganej dokumentacji z zakresu zarządzania cyberbezpieczeństwem;
6. niezapewnienie obsługi incydentu cyberbezpieczeństwa;
7. niezgłoszenie incydentu podlegającego zgłoszeniu do właściwego CSIRT w terminach określonych w przepisach prawa;
8. brak współpracy z właściwym CSIRT lub organem właściwym w trakcie obsługi incydentu;
9. nieusuwanie zidentyfikowanych podatności, które doprowadziły lub mogły doprowadzić do wystąpienia incydentu;
10. niewyznaczenie osoby lub struktury odpowiedzialnej za cyberbezpieczeństwo albo brak zapewnienia wsparcia podmiotu świadczącego usługi z zakresu cyberbezpieczeństwa;
11. nieprzeprowadzanie audytów bezpieczeństwa, jeżeli obowiązek ich przeprowadzenia wynika z przepisów prawa lub decyzji organu właściwego;
12. utrudnianie lub uniemożliwianie przeprowadzenia kontroli przez organ właściwy;
13. niewykonanie zaleceń pokontrolnych w wyznaczonym terminie.

Wysokość administracyjnych kar pieniężnych ustalana jest każdorazowo przez organ właściwy, w granicach określonych w ustawie o krajowym systemie cyberbezpieczeństwa, z uwzględnieniem okoliczności sprawy.

Postanowienia niniejszego rozdziału mają charakter informacyjny i nie zastępują przepisów powszechnie obowiązującego prawa.

Obsługa incydentu



Incydent krytyczny

Incydent cyberbezpieczeństwa powodujący lub mogący powodować poważne skutki dla bezpieczeństwa państwa, porządku publicznego, zdrowia lub życia ludzi, praw i wolności obywatelskich albo funkcjonowania instytucji publicznych, klasyfikowany jako incydent krytyczny przez właściwy zespół CSIRT.

Incydent poważny

Incydent, który powoduje lub może powodować istotne obniżenie jakości albo przerwanie ciągłości działania systemów informatycznych lub realizacji zadań Podmiotu i który podlega zgłoszeniu do właściwego zespołu CSIRT zgodnie z przepisami ustawy o krajowym systemie cyberbezpieczeństwa.

Incydent zwykły

Zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo Podmiotu, jednak nie spełnia kryteriów incydentu poważnego ani krytycznego.

Incydent zwykły nie podlega zgłoszeniu do CSIRT, jednak podlega obowiązkowej obsłudze wewnętrznej, w szczególności rejestracji, analizie oraz podjęciu działań ograniczających jego skutki.

Przekazywanie informacji o zaistniałym incydencie

Informacje o zaistniałym incydencie cyberbezpieczeństwa przekazywane są w sposób zapewniający ochronę poufności, integralności oraz dostępności informacji, z uwzględnieniem obowiązujących przepisów prawa.

1. W przypadku wystąpienia incydentu cyberbezpieczeństwa informacja o incydencie przekazywana jest niezwłocznie do osoby lub komórki organizacyjnej odpowiedzialnej za cyberbezpieczeństwo w Podmiocie.
2. Incydenty zakwalifikowane jako poważne lub krytyczne przekazywane są do właściwego zespołu CSIRT w terminach i w zakresie określonym w ustawie o krajowym systemie cyberbezpieczeństwa.
3. Informacje przekazywane w ramach zgłoszenia incydentu ograniczane są do danych niezbędnych do obsługi incydentu oraz spełnienia obowiązków prawnych, z zachowaniem zasady minimalizacji danych.
4. W przypadku gdy incydent cyberbezpieczeństwa może stanowić naruszenie ochrony danych osobowych, informacja o incydencie przekazywana jest również do Inspektora Ochrony Danych, a dalsze działania podejmowane są zgodnie z procedurą naruszeń ochrony danych osobowych.
5. Informacje o incydencie mogą być przekazywane kierownikowi Podmiotu oraz innym osobom uprawnionym w zakresie niezbędnym do zapewnienia ciągłości działania oraz podjęcia działań naprawczych.
6. Przekazywanie informacji o incydencie do podmiotów zewnętrznych, w tym dostawców usług, organów lub kontrahentów, następuje wyłącznie w zakresie wymaganym przepisami prawa lub niezbędnym do obsługi incydentu.
7. Wszelkie informacje dotyczące incydentów cyberbezpieczeństwa podlegają ochronie i nie mogą być udostępniane osobom nieupoważnionym.

VII. Obowiązki usług cyfrowych

Postanowienia niniejszego rozdziału mają zastosowanie **wyłącznie w przypadku**, gdy Podmiot posiada status dostawcy usługi cyfrowej w rozumieniu przepisów ustawy o krajowym systemie cyberbezpieczeństwa.

1. Obowiązki w zakresie bezpieczeństwa

Dostawca usługi cyfrowej zobowiązany jest do stosowania odpowiednich i proporcjonalnych środków technicznych oraz organizacyjnych, mających na celu zarządzanie ryzykiem cyberbezpieczeństwa systemów informatycznych wykorzystywanych do świadczenia usługi cyfrowej.

Środki te powinny zapewniać poziom bezpieczeństwa adekwatny do istniejącego ryzyka i obejmować w szczególności:

1. bezpieczeństwo systemów informatycznych oraz infrastruktury technicznej wykorzystywanej do świadczenia usługi,
2. zasady postępowania w przypadku wystąpienia incydentu cyberbezpieczeństwa,
3. zapewnienie ciągłości działania usługi cyfrowej, w tym możliwość przywrócenia jej funkcjonowania,
4. monitorowanie, nadzór oraz okresową ocenę skuteczności stosowanych zabezpieczeń.

2. Monitorowanie i ciągłość świadczenia usług

Dostawca usługi cyfrowej prowadzi bieżące monitorowanie funkcjonowania systemów informatycznych w zakresie niezbędnym do zapewnienia ciągłości i bezpieczeństwa świadczenia usługi cyfrowej oraz do wykrywania incydentów cyberbezpieczeństwa.

VIII. Obowiązki podmiotów

Podmiot publiczny, o którym mowa w rozdziale IV niniejszego dokumentu, zobowiązany jest do wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, zgodnie z przepisami ustawy o krajowym systemie cyberbezpieczeństwa.

Podmiot publiczny zobowiązany jest w szczególności do:

a) zapewnienia zarządzania incydentami cyberbezpieczeństwa w swojej jednostce,
b) zgłaszania incydentów podlegających zgłoszeniu do właściwego zespołu CSIRT, niezwłocznie po ich wykryciu, w terminach i zakresie określonych w przepisach prawa,
c) zapewnienia obsługi incydentu cyberbezpieczeństwa we własnej jednostce, w tym podejmowania działań niezbędnych do ograniczenia jego skutków,
d) współpracy z właściwymi organami oraz zespołami CSIRT w zakresie obsługi incydentów, w tym przekazywania niezbędnych informacji,
e) zapewnienia dostępu do informacji o zagrożeniach cyberbezpieczeństwa dla użytkowników i interesariuszy, w zakresie adekwatnym do realizowanych zadań publicznych, w szczególności poprzez publikację stosownych informacji na stronie internetowej Podmiotu.

2. Obowiązki ogólne każdego podmiotu

Każdy podmiot objęty niniejszą procedurą zobowiązany jest do podejmowania działań mających na celu zapewnienie bezpieczeństwa systemów informatycznych, w szczególności poprzez:

a) okresową weryfikację poziomu bezpieczeństwa aplikacji i systemów informatycznych, w których przetwarzane są dane,
b) ocenę ryzyka utraty danych oraz dostępności systemów informatycznych
c) zapewnienie możliwości odtworzenia danych w przypadku ich utraty lub uszkodzenia,
d) ocenę ryzyka nieuprawnionego ujawnienia informacji, w tym informacji stanowiących tajemnicę prawnie chronioną,
e) weryfikację czy dane osobowe powierzone lub przetwarzane przez Podmiot są zabezpieczone w sposób adekwatny do zidentyfikowanych zagrożeń.

IX. Zasady udostępniania informacji i przetwarzania danych osobowych

Przekazywanie oraz udostępnianie informacji związanych z incydentami cyberbezpieczeństwa oraz przetwarzaniem danych osobowych odbywa się z poszanowaniem zasad poufności, integralności i minimalizacji danych, zgodnie z przepisami prawa.

1. Osoba wyznaczona do utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz kierownik Podmiotu zapewniają realizację obowiązków informacyjnych wynikających z przepisów o ochronie danych osobowych, w szczególności rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO).
2. Na stronie internetowej Podmiotu publikowane są informacje wymagane przepisami prawa, w tym w szczególności:

- dane kontaktowe administratora danych osobowych, a w przypadku wyznaczenia Inspektora Ochrony Danych – również dane kontaktowe IOD,
- cele przetwarzania danych osobowych oraz podstawy prawne ich przetwarzania,
- kategorie przetwarzanych danych osobowych,
- informacje o odbiorcach lub kategoriach odbiorców danych osobowych,
- okres przechowywania danych osobowych lub kryteria jego ustalania,
- informacje o prawach osób, których dane dotyczą, w tym o prawie dostępu do danych, ich sprostowania, ograniczenia przetwarzania, wniesienia sprzeciwu oraz wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych,
- informacje o źródle pochodzenia danych osobowych – jeżeli dane nie zostały pozyskane bezpośrednio od osoby, której dane dotyczą.

4. Informacje dotyczące incydentów cyberbezpieczeństwa nie są publikowane publicznie, chyba że obowiązek taki wynika z przepisów prawa lub jest niezbędny do realizacji obowiązków informacyjnych wobec osób, których dane dotyczą.
5. Przetwarzanie danych osobowych w związku z obsługą incydentów cyberbezpieczeństwa odbywa się wyłącznie w zakresie niezbędnym do realizacji obowiązków prawnych Podmiotu oraz z zachowaniem odpowiednich środków technicznych i organizacyjnych.

Załącznik 1

OSOBA ODPOWIEDZIALNA ZA UTRZYMYWANIE KONTAKTÓW Z PODMIOTAMI KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

Przedszkole Nr 4 "Pod zielonym listkiem"
ul. Z. Padlewskiego 3
09-100 Płońsk

……

działając na podstawie art. 21 ustawy z 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (Dz.U.2024.1077) Dyrektor jest osobą wyznaczoną do pełnienia funkcji osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, w szczególności z właściwymi zespołami CSIRT, w zakresie związanym z obsługą incydentów cyberbezpieczeństwa oraz współpracą wynikającą z przepisów prawa.

mgr Barbara Kostrzewa

……

Dyrektor Przedszkola

……

(zajmowane stanowisko służbowe)

Zakres odpowiedzialności osoby powołanej obejmuje w szczególności:

- utrzymywanie kontaktów z właściwymi zespołami CSIRT,
- udział w obsłudze i koordynacji działań związanych z incydentami cyberbezpieczeństwa,
- przekazywanie informacji wymaganych przepisami prawa,
- współpracę z kierownikiem jednostki oraz innymi osobami odpowiedzialnymi za bezpieczeństwo informacji.

ENIGMA

Podpisany elektronicznie przez
Barbara Renata Kostrzewa
09.03.2026
9:39:42 +01'00'

……

Podpis

Załącznik 2

IDENTYFIKACJA INCYDENTU ISTOTNEGO MAJĄCEGO WPŁYW NA CIĄGŁOŚĆ DZIAŁANIA PODMIOTU

Lp.	Zakres informacji	Opis / do uzupełnienia
1	Nazwa podmiotu / jednostki	
2	Osoba zgłaszająca (imię i nazwisko, stanowisko)	
3	Data i godzina zgłoszenia	
4	System / obszar objęty incydentem (aplikacja, system, infrastruktura IT)	
5	Opis incydentu (co się wydarzyło)	
6	Data i godzina wystąpienia incydentu	
7	Data i godzina wykrycia incydentu	
8	Czas trwania incydentu (jeżeli znany)	
9	Zasięg incydentu (komórki organizacyjne, stanowiska, użytkownicy)	
10	Skutki incydentu (np. brak dostępu, zakłócenie pracy, utrata danych)	
11	Wpływ incydentu na realizację zadań Podmiotu	
12	Podjęte działania (doraźne / naprawcze / ograniczające skutki)	
13	Wstępna kwalifikacja incydentu	☐ incydent zwykły ☐ incydent poważny ☐ incydent krytyczny
14	Czy incydent może dotyczyć danych osobowych?	☐ TAK ☐ NIE
15	Jeżeli TAK – data przekazania do IOD	
16	Uwagi dodatkowe	
17	Podpis osoby sporządzającej	
18	Data sporządzenia	

Załącznik 3

ZGŁOSZENIE INCYDENTU CYBERBEZPIECZEŃSTWA DO WŁAŚCIWEGO ZESPOŁU CSIRT

Lp.	Zakres informacji	Opis / do uzupełnienia
1	Nazwa podmiotu / jednostki	
2	Forma organizacyjno-prawna	
3	Adres siedziby	
4	Dane kontaktowe podmiotu (tel., e-mail)	
5	Osoba dokonująca zgłoszenia (imię, nazwisko, stanowisko)	
6	Dane kontaktowe osoby zgłaszającej	
7	Osoba uprawniona do składania wyjaśnień (jeżeli inna)	
8	Dane kontaktowe osoby uprawnionej	
9	Data i godzina wystąpienia incydentu	
10	Data i godzina wykrycia incydentu	
11	Czas trwania incydentu (jeżeli znany)	
12	System / aplikacja / infrastruktura, której dotyczy incydent	
13	Zasięg incydentu (komórki, użytkownicy, obszar)	
14	Liczba osób / użytkowników, których dotyczy incydent	
15	Opis incydentu (przebieg zdarzenia)	
16	Przyczyna lub prawdopodobna przyczyna incydentu	
17	Skutki incydentu dla systemów informatycznych	
18	Wpływ incydentu na realizację zadań Podmiotu	

Lp.	Zakres informacji	Opis / do uzupełnienia
19	Czy incydent może mieć charakter transgraniczny	☐ TAK ☐ NIE
20	Działania podjęte niezwłocznie po wykryciu incydentu	
21	Działania naprawcze	
22	Działania zapobiegawcze	
23	Czy incydent dotyczy danych osobowych	☐ TAK ☐ NIE
24	Jeżeli TAK – data przekazania informacji do IOD	
25	Klasyfikacja incydentu	☐ zwykły ☐ poważny ☐ krytyczny
26	Inne istotne informacje	
27	Data zgłoszenia do CSIRT	
28	Podpis osoby dokonującej zgłoszenia	

Załącznik 4

WERYFIKACJA POZIOMU BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH

w
Przedszkole Nr 4 "Pod zielonym listkiem"

ul. Z. Padlewskiego 3

09-100 Płońsk

Data weryfikacji: 03.03.2026 r.

.

1. APLIKACJE

Lp.	Zakres weryfikacji	TAK / NIE / N/D	Uwagi / wnioski
1.1	Czy dostawcy systemów (np. e-dziennik, sekretariat, księgowość) dbają o bezpieczeństwo swoich aplikacji?	☒ ☐ ☐	Systemy dostarczane przez renomowanych dostawców, aktualizowane zgodnie z harmonogramem
1.2	Czy szkoła reaguje na zgłaszane problemy techniczne i bezpieczeństwa w systemach?	☒ ☐ ☐	Zgłoszenia obsługiwane na bieżąco
1.3	Czy informatyk okresowo sprawdza, czy systemy działają poprawnie i bezpiecznie?	☒ ☐ ☐	Prowadzony bieżący nadzór techniczny
1.4	Czy przy wdrażaniu nowych programów zwraca się uwagę na bezpieczeństwo danych?	☒ ☐ ☐	Analiza przed wdrożeniem
1.5	Czy każdy pracownik ma własne login i hasło do systemów?	☒ ☐ ☐	Indywidualne konta użytkowników
1.6	Czy programy i systemy są na bieżąco aktualizowane?	☒ ☐ ☐	Aktualizacje systemowe i aplikacyjne

2. INFRASTRUKTURA IT

Lp.	Zakres weryfikacji	TAK / NIE / N/D	Uwagi / wnioski
2.1	Czy sprzęt komputerowy i sieć szkolna są pod stałą opieką informatyka?	☒ ☐ ☐	Stała opieka informatyczna
2.2	Czy komputery i urządzenia są zabezpieczone hasłami?	☒ ☐ ☐	Hasła użytkowników i administratora
2.3	Czy szkoła nie udostępnia sieci każdemu bez kontroli (np. hasło do Wi-Fi nie jest publiczne)?	☒ ☐ ☐	Hasło zmieniane okresowo
2.4	Czy sieć szkolna posiada podstawowe zabezpieczenia (np. router, firewall)?	☒ ☐ ☐	Router, firewall
2.5	Czy na komputerach jest antywirus i aktualizacje systemu?	☒ ☐ ☐	Ochrona antywirusowa aktywna
2.6	Czy serwer / ważny sprzęt IT znajduje się w zamkniętym pomieszczeniu?	☒ ☐ ☐	Ograniczony dostęp

3. CZYNNIK LUDZKI I ORGANIZACJA

Lp.	Zakres weryfikacji	TAK / NIE / N/D	Uwagi / wnioski
3.1	Czy w szkole są ustalone zasady dotyczące bezpieczeństwa danych i komputerów?	☒ ☐ ☐	Uregulowane w dokumentacji
3.2	Czy szkoła stosuje podstawowe wymagania dotyczące ochrony danych i bezpieczeństwa informacji (RODO, KRI)?	☒ ☐ ☐	Dokumentacja wdrożona
3.3	Czy pracownicy byli szkoleni z ochrony danych i bezpiecznego korzystania z komputerów?	☒ ☐ ☐	Szkolenia okresowe
3.4	Czy pracownicy wiedzą, że nie należy otwierać podejrzanych maili i linków?	☒ ☐ ☐	Świadomość zagrożeń
3.5	Czy ktoś na bieżąco reaguje, gdy pojawiają się problemy z komputerami lub bezpieczeństwem?	☒ ☐ ☐	Zgłoszenia obsługiwane na bieżąco

Lp.	Zakres weryfikacji	TAK / NIE / N/D	Uwagi / wnioski
3.6	Czy wiadomo, co należy zrobić, gdy dojdzie do incydentu (np. wirus, wyciek danych)?	☒ ☐ ☐	Procedura incydentów

4. WNIOSKI Z WERYFIKACJI

Obszar	*Liczba odpowiedzi TAK*	*Liczba odpowiedzi NIE*	*Liczba odpowiedzi N/D*
Aplikacje	*6*	*0*	*0*
Infrastruktura IT	*6*	*0*	*0*
Czynnik ludzki i organizacja	*6*	*0*	*0*
RAZEM	*18*	*0*	*0*

Poziom	Kryterium (liczba odpowiedzi TAK)
Wysoki	14–18 odpowiedzi TAK
Średni	8–13 odpowiedzi TAK
Niski	0–7 odpowiedzi TAK

Wynik końcowy
Łączna liczba odpowiedzi TAK: 18
Oceniony poziom bezpieczeństwa: ☒Wysoki ☐ Średni ☐ Niski

Załącznik 5

OCENA RYZYKA UTRATY DANYCH

W każdym wierszu należy zaznaczyć jedną odpowiedź, która najlepiej odzwierciedla realne ryzyko w danej placówce.

Zagrożenie	**Wystąpiło**	**Może wystąpić**	**Możliwe**	**Raczej nie**	**Nie wystąpi**	**Nie dotyczy**
Awaria sprzętu, zalanie, przegrzanie, zniszczenie	☐	☐	☒	☐	☐	☐
Awaria sprzętu w wyniku nieautoryzowanych modyfikacji	☐	☐	☐	☒	☐	☐
Kradzież lub zagubienie telefonu, laptopa, nośnika danych	☐	☐	☒	☐	☐	☐
Włamanie do systemu lub urządzenia i usunięcie danych	☐	☐	☐	☒	☐	☐
Zaszyfrowanie danych (ransomware)	☐	☐	☐	☒	☐	☐
Przypadkowe usunięcie danych (błąd ludzki)	☐	☐	☒	☐	☐	☐
Celowe usunięcie danych (działanie umyślne)	☐	☐	☐	☒	☐	☐
Usunięcie danych przez administratora / skrypt / aplikację	☐	☐	☐	☒	☐	☐
Utrata klucza, hasła, PIN-u lub mechanizmu szyfrującego	☐	☐	☐	☒	☐	☐

Podsumowanie ilościowe:

Kategoria	**Łączna liczba wskazań**
Wystąpiło	0
Może wystąpić	0
Możliwe	3
Raczej nie	6
Nie wystąpi	0

Kategoria	Łączna liczba wskazań
Nie dotyczy	0

Interpretacja ryzyka (klucz audytowy)

Wynik oceny (z tabeli zliczającej)	Poziom ryzyka	Wymagane działania
Co najmniej jedno wskazanie w kolumnie „Wystąpiło", „Może wystąpić" lub „Możliwe"	Ryzyko średnie lub wysokie	Należy zaplanować i wdrożyć działania zapobiegawcze lub ograniczające ryzyko
Wskazania wyłącznie w kolumnach „Raczej nie" lub „Nie wystąpi"	Ryzyko niskie	Monitorować ryzyko i okresowo weryfikować poziom zabezpieczeń
Wskazania wyłącznie w kolumnie „Nie dotyczy"	Poza zakresem oceny	Brak konieczności podejmowania działań, brak wpływu na ocenę ryzyka

WYNIK KOŃCOWY OCENY RYZYKA – INTERPRETACJA

Na podstawie przeprowadzonej oceny ryzyka utraty danych stwierdzono wystąpienie wskazań w kolumnach **„Możliwe"** oraz **„Raczej nie"**, przy jednoczesnym braku wskazań w kolumnie **„Wystąpiło"**.

Zgodnie z przyjętym kluczem audytowym oznacza to **ryzyko na poziomie średnim**, które mieści się w **akceptowalnym poziomie dla Podmiotu publicznego**, przy założeniu utrzymywania i doskonalenia stosowanych środków organizacyjnych oraz technicznych.

W związku z powyższym:

- nie zachodzi konieczność podejmowania działań nadzwyczajnych,
- rekomenduje się kontynuowanie monitorowania ryzyka,
- wskazane jest utrzymywanie działań zapobiegawczych, w szczególności w obszarze bezpieczeństwa systemów informatycznych oraz świadomości pracowników.

Załącznik 6

OCENA MOŻLIWOŚCI ODTWORZENIA DANYCH I CIĄGŁOŚCI DZIAŁANIA

W każdym wierszu należy zaznaczyć jedną odpowiedź, która najlepiej odzwierciedla realne ryzyko w danej placówce.

Zdarzenie / zagrożenie	**Wystąpiło**	**Może wystąpić**	**Możliwe**	**Raczej nie**	**Nie wystąpi**	**Nie dotyczy**
Błąd aplikacji, praca w aplikacjach tymczasowych	☐	☐	☒	☐	☐	☐
Awaria zasilania lub sieci, utrata niezapisanych zmian	☐	☐	☒	☐	☐	☐
Awaria sprzętu, zalanie, przegrzanie, zniszczenie	☐	☐	☒	☐	☐	☐
Awaria sprzętu w wyniku nieautoryzowanych modyfikacji	☐	☐	☐	☒	☐	☐
Kradzież lub zagubienie telefonu, laptopa, nośnika danych	☐	☐	☐	☒	☐	☐
Włamanie do sieci lub urządzeń i usunięcie danych	☐	☐	☐	☒	☐	☐
Zaszyfrowanie danych (np. ransomware)	☐	☐	☐	☒	☐	☐
Przypadkowe usunięcie danych (błąd, pośpiech)	☐	☐	☒	☐	☐	☐
Usunięcie danych w celu zwolnienia przestrzeni	☐	☐	☐	☒	☐	☐
Celowe usunięcie danych (zacieranie śladów, treści nielegalne)	☐	☐	☐	☒	☐	☐
Usunięcie danych przez administratora / skrypt / aplikację	☐	☐	☐	☒	☐	☐
Utrata klucza, hasła, PIN-u lub mechanizmu szyfrującego	☐	☐	☐	☒	☐	☐

Podsumowanie ilościowe:

Kategoria	Łączna liczba wskazań
Wystąpiło	0
Może wystąpić	0
Możliwe	4
Raczej nie	8
Nie wystąpi	0
Nie dotyczy	0

Interpretacja wyników

Wynik oceny	Ocena ryzyka	Wymagane działania
Co najmniej jedno wskazanie: „Wystąpiło", „Może wystąpić" lub „Możliwe"	Ryzyko **średnie lub wysokie**	Wymagane działania zapewniające możliwość odtworzenia danych i ciągłość działania
Wskazania wyłącznie: „Raczej nie" lub „Nie wystąpi"	Ryzyko **niskie**	Monitorować i okresowo weryfikować zabezpieczenia
Wskazania wyłącznie: „Nie dotyczy"	Poza zakresem oceny	Brak konieczności działań

WYNIK KOŃCOWY OCENY – INTERPRETACJA

Na podstawie przeprowadzonej oceny stwierdza się, że w Podmiocie nie wystąpiły zdarzenia skutkujące trwałą utratą danych ani przerwą w ciągłości działania. Zidentyfikowane zagrożenia mają charakter potencjalny i mieszczą się w przewidywalnym ryzyku funkcjonowania systemów informatycznych w jednostce publicznej.

Wskazania w kategorii „Możliwe" dotyczą zdarzeń typowych dla środowiska informatycznego (np. awarie zasilania, błędy użytkowników), dla których stosowane są rozwiązania ograniczające skutki, w szczególności wykonywanie kopii zapasowych oraz nadzór informatyczny.

Ocena wskazuje na **ryzyko średnie, akceptowalne**, pod warunkiem utrzymania stosowanych zabezpieczeń oraz okresowej weryfikacji procedur odtwarzania danych i zapewnienia ciągłości działania.

Załącznik 7

OCENA RYZYKA NIEUPRAWIONEGO UJAWNIENIA INFORMACJI PRAWNI CHRONIONYCH

W każdym wierszu należy zaznaczyć jedną odpowiedź, która najlepiej odzwierciedla realne ryzyko w danej placówce

Tabela oceny ryzyka ujawnienia tajemnicy

Zdarzenie / zagrożenie	Wystąpiło	Może wystąpić	Możliwe	Raczej nie	Nie wystąpi	Nie dotyczy
Kradzież lub zagubienie telefonu, laptopa lub nośnika danych	☐	☐	☐	☒	☐	☐
Przypadkowe udostępnienie danych na nośniku z innymi danymi	☐	☐	☒	☐	☐	☐
Sprzedaż lub utylizacja nośnika bez bezpiecznego usunięcia danych	☐	☐	☐	☒	☐	☐
Włamanie do sieci lub urządzeń	☐	☐	☐	☒	☐	☐
Infekcja złośliwym oprogramowaniem (malware, spyware)	☐	☐	☐	☒	☐	☐
Nieuprawniony dostęp do konta e-mail, serwera lub zasobów sieciowych	☐	☐	☐	☒	☐	☐
Wyciek danych wskutek błędu lub awarii po stronie dostawcy usług	☐	☐	☐	☒	☐	☐
Udostępnienie danych e-mailem do nieprawidłowego odbiorcy (DW/UDW)	☐	☐	☒	☐	☐	☐
Udostępnienie danych przez komunikator (zły kanał / grupa)	☐	☐	☐	☒	☐	☐

Zagrożenia wynikające z zachowań użytkowników

Zdarzenie / zagrożenie	Wystąpiło	Może wystąpić	Możliwe	Raczej nie	Nie wystąpi	Nie dotyczy
Udostępnienie danych poprzez niezabezpieczony link („głębokie ukrycie”)	☐	☐	☒	☐	☐	☐
Celowe ujawnianie informacji w celu zwrócenia uwagi (media, social media)	☐	☐	☐	☒	☐	☐
Nieświadome publikowanie informacji w publicznych zasobach sieci	☐	☐	☐	☒	☐	☐
Reakcja na próby wyłudzeń (phishing, vishing, smishing)	☐	☐	☒	☐	☐	☐

Podsumowanie ilościowe:

Kategoria	Łączna liczba wskazań
Wystąpiło	0
Może wystąpić	0
Możliwe	4
Raczej nie	9
Nie wystąpi	0
Nie dotyczy	0

Interpretacja wyników

Wynik oceny	Poziom ryzyka	Wymagane działania
Co najmniej jedno wskazanie: „Wystąpiło”, „Może wystąpić” lub „Możliwe”	Ryzyko **średnie lub wysokie**	Wdrożyć działania organizacyjne i techniczne ograniczające ryzyko ujawnienia
Wskazania wyłącznie: „Raczej nie” lub „Nie wystąpi”	Ryzyko **niskie**	Monitorować i okresowo weryfikować zabezpieczenia
Wskazania wyłącznie: „Nie dotyczy”	Poza zakresem oceny	Brak konieczności działań

WYNIK KOŃCOWY – INTERPRETACJA OPISOWA

Na podstawie przeprowadzonej oceny ryzyka stwierdza się, że w Podmiocie nie wystąpiły przypadki nieuprawnionego ujawnienia informacji prawnie chronionych. Zidentyfikowane zagrożenia mają charakter potencjalny i dotyczą przede wszystkim ryzyk wynikających z błędów ludzkich oraz powszechnych zagrożeń teleinformatycznych.

Zastosowane w Podmiocie środki organizacyjne i techniczne, w tym procedury ochrony informacji, zabezpieczenia systemowe oraz działania podnoszące świadomość pracowników, ograniczają prawdopodobieństwo wystąpienia nieuprawnionego ujawnienia informacji.

Ocena wskazuje na **ryzyko średnie, akceptowalne**, wymagające dalszego monitorowania oraz utrzymywania i doskonalenia stosowanych zabezpieczeń.

Załącznik 8

WERYFIKACJA POZIOMU ZABEZPIECZEŃ
DANYCH POWIERZONYCH PRZEZ PODMIOTY TRZECIE

W każdym wierszu należy zaznaczyć jedną odpowiedź, która najlepiej odzwierciedla realne ryzyko w danej placówce.

Tabela – dane powierzone

Zdarzenie / zagrożenie	**Wystąpiło**	**Może wystąpić**	**Możliwe**	**Raczej nie**	**Nie wystąpi**	**Nie dotyczy**
Kradzież lub zagubienie służbowych nośników (telefon, laptop, pendrive, dysk)	☐	☐	☐	☒	☐	☐
Przypadkowe udostępnienie danych na zewnętrznych nośnikach	☐	☐	☒	☐	☐	☐
Przetwarzanie danych na prywatnym, niezabezpieczonym nośniku	☐	☐	☐	☒	☐	☐
Przetwarzanie danych na służbowym sprzęcie bez zabezpieczeń przed utratą danych	☐	☐	☐	☒	☐	☐
Utylizacja lub sprzedaż nośnika bez bezpiecznego usunięcia danych (także dokumenty papierowe)	☐	☐	☐	☒	☐	☐
Włamanie do służbowej sieci lub systemów informatycznych	☐	☐	☐	☒	☐	☐
Włamanie do systemów podczas pracy zdalnej (home office)	☐	☐	☐	☒	☐	☐
Infekcja złośliwym oprogramowaniem służbowej sieci lub urządzeń	☐	☐	☐	☒	☐	☐

Tabela – Zagrożenia związane z pracą zdalną i zachowaniami użytkowników

Zdarzenie / zagrożenie	Wystąpiło	Może wystąpić	Możliwe	Raczej nie	Nie wystąpi	Nie dotyczy
Infekcja służbowego sprzętu w sieci domowej pracownika	☐	☐	☒	☐	☐	☐
Nieuprawniony dostęp do służbowego konta w usłudze internetowej	☐	☐	☐	☒	☐	☐
Włamanie do sieci służbowej z wykorzystaniem dostępu zdalnego	☐	☐	☐	☒	☐	☐
Udostępnienie danych e-mailem do błędnego odbiorcy (DW/UDW)	☐	☐	☒	☐	☐	☐
Udostępnienie danych przez komunikator (zły kanał / grupa)	☐	☐	☐	☒	☐	☐
Udostępnienie danych poprzez niezabezpieczony link („głębokie ukrycie”)	☐	☐	☒	☐	☐	☐
Umieszczanie danych w publicznych lub niezabezpieczonych zasobach Internetu	☐	☐	☐	☒	☐	☐
Reakcja na próby wyłudzeń (phishing, vishing, smishing)	☐	☐	☒	☐	☐	☐

Podsumowanie ilościowe:

Kategoria	Łączna liczba wskazań
Wystąpiło	0
Może wystąpić	0
Możliwe	4
Raczej nie	12
Nie wystąpi	0
Nie dotyczy	0

Interpretacja wyników

Wynik oceny	**Poziom ryzyka**	**Wymagane działania**
Co najmniej jedno wskazanie: „Wystąpiło”, „Może wystąpić” lub „Możliwe”	Ryzyko **średnie lub wysokie**	Wdrożyć dodatkowe środki techniczne i organizacyjne
Wskazania wyłącznie: „Raczej nie” lub „Nie wystąpi”	Ryzyko **niskie**	Monitorować i okresowo weryfikować zabezpieczenia
Wskazania wyłącznie: „Nie dotyczy”	Poza zakresem oceny	Brak konieczności działań

WYNIK KOŃCOWY – INTERPRETACJA OPISOWA

Na podstawie przeprowadzonej weryfikacji stwierdza się, że dane powierzone przez podmioty trzecie są przetwarzane z zachowaniem wymaganych środków organizacyjnych i technicznych. Nie odnotowano zdarzeń skutkujących naruszeniem bezpieczeństwa danych powierzonych.

Zidentyfikowane zagrożenia mają charakter potencjalny i dotyczą głównie ryzyk wynikających z błędów użytkowników oraz specyfiki pracy zdalnej. Ryzyka te są ograniczane poprzez stosowane procedury, zabezpieczenia systemowe oraz działania podnoszące świadomość pracowników.

Ocena wskazuje na **ryzyko średnie, akceptowalne**, wymagające dalszego monitorowania oraz utrzymywania i okresowej weryfikacji stosowanych zabezpieczeń.