Zarządzenie nr 14/2025
Dyrektora Centrum Obsługi
Placówek Opiekuńczo-Wychowawczych w Wydrznie
z dnia 2 lipca 2025 r.

w sprawie wprowadzenia Procedury zarządzania incydentami związanymi z cyberbezpieczeństwem i bezpieczeństwem informacji w Centrum Obsługi Placówek Opiekuńczo-Wychowawczych w Wydrznie i jednostkach obsługiwanych tj. Placówce Opiekuńczo-Wychowawczej Nr 1 w Wydrznie, Placówce Opiekuńczo-Wychowawczej Nr 2 w Wydrznie i Placówce Opiekuńczo-Wychowawczej Nr 3 w Łasinie

Na podstawie art. 22 ust.1 pkt 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077, z późn.zm.) oraz §12 pkt 9 Regulaminu Organizacyjnego Centrum Obsługi Placówek Opiekuńczo-Wychowawczych w Wydrznie, stanowiącego załącznik do Uchwały Nr 57/109/2020 Zarządu Powiatu Grudziądzkiego z dnia 2 grudnia 2020 r., zmienionego Uchwałą Nr 100/97/2021 Zarządu Powiatu Grudziądzkiego z dnia 24 listopada 2021 r., **zarządzam co następuje**:

§ 1

Wprowadzam Procedurę zarządzania incydentami związanymi z cyberbezpieczeństwem i bezpieczeństwem informacji w Centrum Obsługi Placówek Opiekuńczo-Wychowawczych w Wydrznie i jednostkach obsługiwanych tj. Placówce Opiekuńczo-Wychowawczej Nr 1 w Wydrznie, Placówce Opiekuńczo-Wychowawczej Nr 2 w Wydrznie i Placówce Opiekuńczo-Wychowawczej Nr 3 w Łasinie, stanowiącą załącznik do niniejszego zarządzenia.

§ 2

Zobowiązuję pracowników jednostek wymienionych w § 1 – bez względu na zajmowane stanowisko – do zapoznania się z Procedurą zarządzania incydentami związanymi z cyberbezpieczeństwem i bezpieczeństwem informacji, celem bezwzględnego przestrzegania jej postanowień.

§ 3

Zobowiązuję koordynatorów jednostek obsługiwanych, o których mowa w § 1, do zapoznania pracowników z Procedurą zarządzania incydentami związanymi z cyberbezpieczeństwem i bezpieczeństwem informacji, celem bezwzględnego przestrzegania postanowień dokumentu.

§ 4

Nadzór nad wykonaniem zarządzenia powierzam Panu Dawidowi Banasiak - informatykowi.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Centrum Obsługi Placówek
Opiekuńczo-Wychowawczych w Wydrznie
Izabela Kotlewska

Załącznik do Zarządzenia Nr 14/2025
Dyrektora Centrum Obsługi
Placówek Opiekuńczo-Wychowawczych
w Wydrznie z dnia 2 lipca 2025 r.

PROCEDURA ZARZĄDZANIA INCYDENTAMI ZWIĄZANYMI Z CYBERBEZPIECZEŃSTWEM I BEZPIECZEŃSTWEM INFORMACJI W CENTRUM OBSŁUGI PLACÓWEK OPIEKUŃCZO-WYCHOWAWCZYCH W WYDRZNIE I JEDNOSTKACH OBSŁUGIWANYCH tj. PLACÓWCE OPIEKUŃCZO-WYCHOWAWCZEJ NR 1 W WYDRZNIE, PLACÓWCE OPIEKUŃCZO-WYCHOWAWCZEJ NR 2 W WYDRZNIE, PLACÓWCE OPIEKUŃCZO-WYCHOWAWCZEJ NR 3 W ŁASINIE

I. Postanowienia ogólne

§ 1

1. Procedura zarządzania incydentami związanymi z cyberbezpieczeństwem i bezpieczeństwem informacji ma na celu zapewnienie ciągłości operacyjnej oraz ograniczenie wpływu przypadków naruszeń bezpieczeństwa zasobów informacyjnych na działalność Centrum Obsługi Placówek Opiekuńczo-Wychowawczych w Wydrznie i jednostek obsługiwanych.
2. Podstawą prawną do opracowania i wdrożenia niniejszej Procedury jest:
   a) art. 22 ust.1 pkt. 1 ustawy o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r. (Dz. U. z 2024 r. poz. 1077);
   b) § 19 ust. 2 pkt 13 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 (Dz. U. z 2024 r. poz. 773);
   c) 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/ (Dz. Urz. UE L 119 z 4 maja 2016 r.), zwanym dalej „RODO".

II. Objaśnienie terminów

§ 2

Ilekroć w Procedurze jest mowa o:

1) **Centrum** – należy przez to rozumieć Centrum Obsługi Placówek Opiekuńczo-Wychowawczych w Wydrznie z siedzibą w Wydrznie, Wydrzno13/1, 86-320 Łasin; tel. 56 468 93 07, adres poczty e-mail: sekretariat@copow-wydrzno.pl; identyfikator ePuap: COPOWWydrzno, e-Doręczenia: AE:PL-13852-22400-JBGJH-30;
2) **Jednostkach obsługiwanych** – należy przez to rozumieć:
   - Placówkę Opiekuńczo-Wychowawczą Nr 1 w Wydrznie z siedzibą Wydrzno 13/2, 86-320 Łasin, tel. 504 329 673,
   - Placówkę Opiekuńczo-Wychowawczą Nr 2 w Wydrznie z siedzibą Wydrzno 13/3, 86-320 Łasin, tel. 504 329 674,
   - Placówkę Opiekuńczo-Wychowawczą Nr 3 w Łasinie z siedzibą 86-320 Łasin, ul. Odrodzenia Polski 3A, tel. 56 468 13 78;
3) **Cyberbezpieczeństwo** – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;
4) **Incydent** – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo;

5) **Incydent cyberbezpieczeństwa** – zbiorcza nazwa obejmująca incydent, incydent w podmiocie publicznym, incydent krytyczny;
6) **Incydent w podmiocie publicznym** – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny;
7) **Incydent krytyczny** – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku prawnego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw lub wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT NASK;
8) **Zagrożenie cyberbezpieczeństwa** – potencjalna przyczyna wystąpienia incydentu;
9) **Administrator Systemów Informatycznych** – osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za sprawność i konserwacje oraz wdrażanie technicznych zabezpieczeń systemów informatycznych zwany dalej „ASI";
10) **Administrator Danych Osobowych** – organ, jednostka organizacyjna, podmiot lub osoba decydujące o celach i środkach przetwarzania danych osobowych. W tym przypadku Administratorem Danych Osobowych jest Centrum Obsługi Placówek Opiekuńczo-Wychowawczych w Wydrznie zwany dalej „ADO";
11) **Inspektor Ochrony Danych** - osoba fizyczna powołana przez Administratora Danych Osobowych, zajmująca się zapewnianiem przestrzegania przepisów o ochronie danych osobowych oraz prowadzeniem dokumentacji związanej z przetwarzaniem danych przez administratora zwany dalej „IOD".

III. Kategorie incydentów

§ 3

1. Incydent cyberbezpieczeństwa i bezpieczeństwa informacji to zdarzenie, którego skutkiem jest lub może być naruszenie bezpieczeństwa aktywów informacyjnych oraz który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny.
2. Przyczyną powstania incydentu cyberbezpieczeństwa może być:
   a) zdarzenie losowe zewnętrzne (np. klęski żywiołowe, pożary, zakłócenia w dostawie energii elektrycznej itp.), którego wystąpienie może spowodować zniszczenie lub uszkodzenie infrastruktury informatycznej albo dokumentacji papierowej oraz zakłócenie ciągłości pracy systemów nie powodując naruszenia poufności danych;
   b) zdarzenie losowe wewnętrzne (np. błędy w oprogramowaniu, awarie sprzętu itp.), które mogą spowodować zakłócenia ciągłości pracy systemów, a także prowadzić do zniszczenia lub utraty danych;
   c) świadome i celowe działania mające na celu naruszenie poufności zasobów informacyjnych, w tym poufności danych.
3. Incydentami cyberbezpieczeństwa w szczególności są takie działania jak:
   a) naruszenie poufności, to jest ujawnienie informacji niepowołanym osobom;
   b) naruszenie integralności, to jest zniszczenie, uszkodzenie lub przekłamanie informacji;
   c) naruszenie dostępności, to jest braku dostępu do danych przez uprawnionych użytkowników.
4. Przyczyny incydentów cyberbezpieczeństwa mogą dotyczyć:
   a) niewłaściwego wykorzystywania zasobów informatycznych lub niewłaściwe postępowanie z dokumentacją papierową;
   b) działania szkodliwego oprogramowania;
   c) próby omijania systemów zabezpieczeń;
   d) nieautoryzowanego dostępu do systemów, aplikacji i dokumentów;
   e) zniszczenie lub kradzież urządzeń wykorzystywanych do przetwarzania i przechowywania informacji;

f) zniszczenie lub kradzieży nośników danych;
g) próby wyłudzeń informacji;
h) ataków socjotechnicznych, ataków z wykorzystaniem technik zagrażających poufności;
i) integralności lub dostępności informacji;
j) nieprawidłowości w zakresie zabezpieczenia przechowywania danych, w tym danych osobowych;
k) naruszenia zasad obowiązujących w Centrum Obsługi Placówek Opiekuńczo-Wychowawczych w Wydrznie i jednostkach obsługiwanych, dotyczących bezpieczeństwa informacji, w tym danych osobowych.

5. O możliwości zaistnienia przypadku naruszenia cyberbezpieczeństwa mogą świadczyć:
   a) nadmierne, w stosunku do wykonywanych zadań (zakresu upoważnienia), uprawnienia użytkownika do zasobów systemu;
   b) niestabilna praca systemu teleinformatycznego;
   c) korzystanie z zasobów systemu poza godzinami pracy (bez zgody przełożonego);
   d) nowe „ podejrzane" (nieznane) konta użytkowników;
   e) wysoka aktywność kont, które długo pozostawały niewykorzystane;
   f) zanotowanie w krótkim czasie dużej liczby nieudanych prób logowania;
   g) anomalie w pracy systemu lub programu (świadczące np. o obecności wirusa komputerowego);
   h) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach, w których następuje przetwarzanie informacji w Centrum Obsługi Placówek Opiekuńczo-Wychowawczych w Wydrznie i jednostkach obsługiwanych (uszkodzone zamki, okna, drzwi, naruszone plomby, itp.).

IV. Zgłaszanie incydentów związanych z cyberbezpieczeństwem i bezpieczeństwem informacji

§ 4

1. W przypadku ujawnienia incydentu (kiedy incydent dotyczy systemów komputerowych) osoba wcześniej zgłoszona do CSIRT NASK, dokonuje takiego zgłoszenia za pomocą formularza internetowego https://incydent.cert.pl/#!/lang=pl,entityType=publicInstitution,publicEssentialService=false,publicInstitutionIncident=true.
   Zgłoszenie należy potwierdzić szczegółową notatką służbową, którą przekazuje się Administratorowi Danych Osobowych osobiście, za potwierdzeniem odbioru.
2. Notatka musi zawierać następujące informacje:
   a) imię i nazwisko osoby zgłaszającej;
   b) stanowisko oraz jednostka zgłaszająca;
   c) dokładne miejsce oraz datę wystąpienia incydentu;
   d) opis incydentu w sposób adekwatny do posiadanej wiedzy i umiejętności zgłaszającego;
   e) informację o zgromadzonych materiałach dowodowych;
   f) informacje dotyczące sposobu postępowania z incydentem.
   Wzór notatki stanowi załącznik nr 1 do niniejszej Procedury.
3. Brak umiejętności poprawnego rozpoznania incydentu przez osobę zgłaszającą nie może być przyczyną zaniechania zgłoszenia.
4. W przypadku nieobecności IOD/ASI incydent należy zgłosić do ADO.
5. W przypadku stwierdzenia incydentu krytycznego lub incydentu w Centrum Obsługi Placówek Opiekuńczo-Wychowawczych w Wydrznie i jednostkach obsługiwanych należy niezwłocznie telefonicznie powiadomić o tym fakcie osobę pełniącą funkcję odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz IOD. W dalszej kolejności należy zgłosić do IOD mailowo i potwierdzić oficjalnym pismem opatrzonym podpisem dyrektora Centrum i jednostek obsługiwanych.

V. Podejmowanie działań w związku ze zgłaszanymi incydentami związanymi z cyberbezpieczeństwem i bezpieczeństwem informacji

§ 5

1. Zgłoszenie incydentu rejestrowane jest przez ASI i przechowywane w teczce ***„Procedura zarządzania incydentami związanymi z cyberbezpieczeństwem i bezpieczeństwem informacji w Centrum Obsługi Placówek Opiekuńczo-Wychowawczych i jednostkach obsługiwanych"***. Osoba zgłaszająca incydent powinna w miarę możliwości zabezpieczyć materiał dowodowy (np. zrzut ekranu monitora, zdjęcie niezabezpieczonych materiałów zawierających dane osobowe itp.). Działania związane z obsługą zdarzenia w pierwszej kolejności dotyczą rozpoznania i kwalifikacji zgłoszenia. W przypadku, kiedy zgłoszenie zakwalifikowane zostało jako incydent cyberbezpieczeństwa lub bezpieczeństwa informacji, dokonywana jest jego ocena istotności. Powyższe działania wykonuje ASI w porozumieniu z IOD oraz informatykiem zatrudnionym w Centrum Obsługi Placówek Opiekuńczo-Wychowawczych w Wydrznie.
2. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:
   a) powstałe szkody będące wynikiem incydentu;
   b) wpływ incydentu na działanie systemów;
   c) wpływ incydentu na ciągłość działania Urzędu;
   d) koszty usunięcia skutków incydentu;
   e) szacowany czas naprawy skutków wywołanych incydentem;
   f) oszacowanie zasobów koniecznych do przywrócenia ciągłości działania systemów.
3. Zakwalifikowanie zgłoszenia incydentu jako „fałszywy alarm" kończy postępowanie, o czym ASI informuje zgłaszającego.
4. W przypadku zakwalifikowania zdarzenia jako incydentu związanego z bezpieczeństwem informacji lub cyberbezpieczeństwem, ASI wspólnie z IOD podejmuje działania zabezpieczające i naprawcze zamierzające do zniwelowania szkód powstałych w wyniku incydentu.
5. O wynikach analizy incydentu oraz podjętych działaniach naprawczych należy poinformować osobę pełniącą funkcję odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa lub IOD, który informuje ADO.
6. W przypadku stwierdzenia incydentu w podmiocie publicznym lub incydentu krytycznego ASI nie później niż w ciągu 24 godzin od momentu wykrycia, zgłasza incydent do właściwego CSIRT NASK (Naukowa i Akademicka Sieć Komputerowa – Państwowego Instytutu Badawczego
   ul. Kolska 12, 01-045 Warszawa).
7. Zgłoszenia do CSIRT NASK przekazywane są w sposób elektroniczny. Procedura zgłoszeń opisana jest pod adresem internetowym https:/incydent.cert.pl.
8. W zgłoszeniu przekazuje się informacje zgodnie z formularzem oraz zgodnie z treścią art. 23 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
9. W przypadku stwierdzenia działań zamierzonych, przy jednoczesnym zidentyfikowaniu oraz incydentu dotyczącego naruszenia bezpieczeństwa informacji sprawcy cyberbezpieczeństwa, ADO podejmuje decyzję dotyczącą wyciągnięcia ewentualnych konsekwencji dyscyplinarnych wobec sprawcy incydentu. Jednocześnie, w zależności od wagi incydentu mogą być powiadomione organy ścigania.

VI. Podejmowanie działań w związku ze zgłaszanymi incydentami naruszenia bezpieczeństwa przetwarzania danych osobowych

§ 6

1. W przypadku naruszenia ochrony danych osobowych mają zastosowanie przepisy art. 33-34 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 – RODO/ (Dz. Urz. UE L 119 z dnia 05 kwietnia 2016 r.).
2. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie ochrony danych osobowych tj.:
   a) przypadkowe lub niezgodne z prawem zniszczenia danych;
   b) przypadkowa lub niezgodna z prawem utrata danych;
   c) przypadkowa lub niezgodna z prawem modyfikacja danych;
   d) nieuprawnione ujawnienie danych;
   e) nieuprawniony dostęp do danych osobowych.
3. Każdy pracownik zatrudniony przy przetwarzaniu danych osobowych, stażysta, praktykant itp. jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie powiadomić o tym fakcie swojego bezpośredniego przełożonego oraz Inspektora Ochrony Danych i Administratora Systemów Informatycznych (jeżeli naruszenie ma związek z systemami informatycznymi).
4. Fakt naruszenia lub podejrzenia ochrony danych osobowych należy potwierdzić pisemnie poprzez niezwłocznie sporządzenie notatki służbowej, w której umieszcza się informacje o dacie, czasie, miejscu, okolicznościach zdarzenia. Notatkę przekazuje się Inspektorowi Ochrony Danych zatrudnionemu w Centrum Obsługi Placówek Opiekuńczo-Wychowawczych w Wydrznie osobiście, za potwierdzeniem odbioru, lub przesyła za pośrednictwem skrzynki pocztowej. Dodatkowo kopię notatki przekazuje się swojemu bezpośredniemu przełożonemu. O zdarzeniu IOD niezwłocznie powiadamia ADO.
5. Zgłoszenia są rejestrowane w **„Rejestrze naruszeń ochrony danych osobowych”** ***(załącznik nr 2)***, prowadzonym zgodnie z art. 33 ust. 5 RODO.
6. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:
   a) charakter naruszenia ochrony danych osobowych;
   b) kategorie i przybliżoną liczbę osób, których dane dotyczą;
   c) kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   d) możliwe konsekwencje naruszenia ochrony danych osobowych;
   e) koszty usunięcia skutków incydentu;
   f) szacowany czas naprawy skutków wywołanych incydentem.
7. Zakwalifikowanie zgłoszenia incydentu jako „fałszywy alarm” kończy postępowanie, o czym IOD informuje zgłaszającego.
8. Sprawdzenie naruszenia lub podejrzenia naruszenia ochrony danych osobowych kończy się sprawozdaniem, które przekazywane jest ADO. Sprawozdanie wykonuje IOD wraz z ASI.
9. W przypadku zakwalifikowania zdarzenia jako naruszenie ochrony danych osobowych, które skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych, ADO bez zbędnej zwłoki, nie później niż w terminie 72 godzin od stwierdzenia naruszenia powiadamia Urząd Ochrony Danych Osobowych.
10. Zgłoszenie do UODO przekazywane są w sposób elektroniczny. Procedura zgłoszeń opisana jest pod adresem internetowym: https://uodo.gov.pl .
11. IOD wraz z ASI podejmuje działania zabezpieczające i naprawcze zmierzające do niwelowania skutków powstałych w wyniku incydentu, jak również działania zaradcze dla uniknięcia wystąpienia podobnych incydentów w przyszłości.
12. Jeżeli zgłoszony incydent naruszania ochrony danych osobowych może spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, a stosowane w Centrum Obsługi Placówek Opiekuńczo-Wychowawczych w Wydrznie techniczne i organizacyjne środki ochrony danych nie eliminują tego ryzyka, IOD bez zbędnej zwłoki informuje ADO o konieczności zawiadamiania osób, których dane dotyczą o takim naruszeniu i przygotowuje stosowane dokumenty do podpisu.

13. Jeżeli zawiadomienie osób, których dane dotyczą wymagałoby dużego wysiłku, IOD przygotowuje publiczny komunikat lub wybiera inny stosowny środek, za pomocą którego zawiadomienie zostanie tym osobom przekazane.
14. W przypadku stwierdzenia działań zamierzonych, przy jednoczesnym zidentyfikowaniu sprawcy incydentu dotyczącego naruszenia bezpieczeństwa przetwarzania danych osobowych, ADO podejmuje decyzję dotyczącą wyciągnięcia ewentualnych konsekwencji dyscyplinarnych wobec sprawcy incydentu. Jednocześnie, w zależności od wagi incydentu, mogą być powiadomione organy ścigania.

Załącznik nr 1
do Procedury Zarządzania
Incydentami związanymi
z cyberbezpieczeństwem
i bezpieczeństwem informacji

NOTATKA SŁUŻBOWA ZE ZGŁOSZENIA INCYDENTÓW ZWIĄZANYCH Z CYBERBEZPIECZEŃSTWEM I BEZPIECZEŃSTWEM INFORMACJI

1. Imię i nazwisko osoby zgłaszającej

   .....

2. Stanowisko oraz jednostka zgłaszająca

   .....

3. Dokładne miejsce oraz data wystąpienia incydentu

   .....

   .....

4. Opis incydentu w sposób adekwatny do posiadanej wiedzy i umiejętności zgłaszającego

   .....

   .....

   .....

5. Informacje o zgromadzonych materiałach dowodowych

   .....

   .....

   .....

6. Informacje dotyczące sposobu postępowania z incydentem

   .....

   .....

   .....

.....
(data i podpis)

Załącznik nr 2
do Procedury Zarządzania
Incydentami związanymi
z cyberbezpieczeństwem
i bezpieczeństwem informacji

REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

Lp.	Rodzaj naruszenia	Obowiązek zgłoszenia organowi	Obowiązek zawiadomienia osoby, której dane dotyczą	Okoliczności naruszenia	Skutki naruszenia	Podjęte działania zaradcze