Polityka Bezpieczeństwa Informacji wprowadzona
Zarządzeniem Dyrektora Zespołu Szkól (…) nr 18/2021

POLITYKA BEZPIECZEŃSTWA INFORMACJI W ZESPOLE SZKÓŁW BYSTRZEJOWICACH PIERWSZYCH IM HELENY BABISZ

Bystrzejowice Pierwsze, 2021

§ 1.
POSTANOWIENIA OGÓLNE

1. Polityka Bezpieczeństwa Informacji określana dalej Polityką jest zbiorem dokumentów, określających metody i zasady zapewnienia bezpieczeństwa informacji w Zespole Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz. Opracowana została z uwzględnieniem wymagań prawnych zawartych m.in. w:

1) Rozporządzeniu 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);
2) ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781);
3) ustawie z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2020 r. poz. 364 ze zm.),
4) ustawie z dnia 6 września 2001 roku o dostępie do informacji publicznej (Dz. U. z 2019 r. poz. 1429),
5) ustawie z dnia z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2020 r. poz. 1173),
6) ustawie z dnia 27 lipca 2001 roku o ochronie baz danych (Dz. U. 2019 poz. 2134 z późn.zm)
7) ustawie z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344.);
8) ustawie z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (Dz. U. z 2019 r. poz. 1231 ze zm.),
9) rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 roku 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 2017 r. poz. 2247),
10) ustawie z dnia 12 marca 2004 roku o pomocy społecznej (dz. U. z 2019 r. poz. 1507 i 1622)

2. Celem wdrożenia przedmiotowej Polityki jest zapewnienie wsparcia i wskazanie wytycznych dla działań na rzecz bezpieczeństwa informacji, prowadzących do spełnienia wymagań prawnych oraz zapewnienia:

- ciągłości działania Szkoły,
- poufności danych wrażliwych,

- dostępności wymaganych informacji.

3. Cele osiągane są przez:
   1) zapewnienie wsparcia Administratora dla Polityki,
   2) właściwą organizację, bazującą na udokumentowanej Polityce Bezpieczeństwa Informacji,
   3) zarządzanie ryzykiem w celu ograniczania go do akceptowalnego poziomu,
   4) właściwą ochronę informacji, a w szczególności informacji prawnie chronionych,
   5) zapewnienie odpowiedniego poziomu dostępności informacji i niezawodności systemów informatycznych,
   6) właściwą ochronę informacji związanych z zawartymi umowami,
   7) wdrażanie, eksploatację i rozwój systemów informacyjnych z zachowaniem zasad bezpieczeństwa,
   8) stałą edukację użytkowników,
   9) okresowe audyty Polityki.
4. Polityka ma zastosowanie również do ochrony procesów przetwarzania danych osobowych zachodzących w działalności Zespołu Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz w celu ich bezpiecznego wykorzystania oraz określa zasady korzystania z systemów informatycznych.
5. Polityka stanowi jeden ze środków organizacyjnych mających na celu wykazanie, że przetwarzanie danych w Zespole Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz odbywa się zgodnie z powyższymi przepisami prawa.
6. Z zasadami w Polityce są zapoznawani wszyscy użytkownicy systemów tradycyjnych i informatycznych, składając odpowiednie oświadczenie.

7.Oświadczenie przechowywane jest w aktach osobowych pracownika, a drugi egzemplarz w dokumentacji IOD.

§ 2.

DEFINICJE

Określenia i skróty użyte w Polityce oznaczają:

1) **Administrator (danych osobowych)**, zwany też **ADO** - Dyrektor Zespołu Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz w świetle art. 4 pkt 7 RODO rozumie się przez to osobę fizyczna lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

2) **Inspektor Ochrony Danych**, zwany też **IOD**- osoba formalnie wyznaczona przez ADO w celu informowania i doradzania ADO/Podmiotowi Przetwarzającemu/ Użytkownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób, których dane są przetwarzane i organu nadzorczego;
3) **Użytkownik** zwany też **użytkownik systemu informatycznego** - osoba zatrudniona w jednostce, posiadająca upoważnienie wydane przez ADO lub uprawnioną przez niego osobę i dopuszczona do przetwarzania danych osobowych w systemie informatycznym;
4) **Użytkownik zewnętrzny –** osoba niezatrudniona w jednostce, której powierzono przetwarzanie danych osobowych w związku z wykonywaniem powierzonych obowiązków;
5) **Aktywo/zasób** *(informacyjny)*– wszystko to, co ma wartość dla organizacji w zakresie informacji *(zarówno informacje, jak i środki techniczne oraz organizacyjne do ich przetwarzania);*
6) **Bezpieczeństwo informacji** – zachowanie poufności, integralności i dostępności informacji;
7) **Dostępność** – zapewnienie, że osoby upoważnione będą miały dostęp do informacji tylko wtedy, gdy jest to uzasadnione;
8) **Incydent związany z bezpieczeństwem informacji**– pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań i zagrażają bezpieczeństwu informacji**;**
9) **Integralność**– właściwość polegająca na zapewnieniu dokładności i kompletności aktywów**;**
10) **Niezawodność** – właściwość oznaczająca spójne zamierzone zachowanie i skutki;
11) **Poufność** – właściwość polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom**;**
12) **Postępowanie z ryzykiem** – proces wyboru i wdrażania środków modyfikujących ryzyko**;**
13) **Ryzyko** – prawdopodobieństwo wystąpienia zagrożenia, które wykorzystując podatność *(podatności)* aktywa, może doprowadzić do jego uszkodzenia lub zniszczenia**;**
14) **Szacowanie ryzyka** – całościowy proces analizy i oceny ryzyka**;**
15) **Zarządzanie ryzykiem** – proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych, przy zachowaniu akceptowalnego poziomu kosztów;

16) **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
17) **System tradycyjny** - zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;
18) **Zabezpieczenie danych w systemie informatycznym** - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

§ 3.
ZAKRES POLITYKI BEZPIECZEŃSTWA INFORMACJI

Zespól Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz obejmuje ustanawianie, wdrażanie, eksploatację, monitorowanie, utrzymywanie i doskonalenie bezpieczeństwa informacji. Zakresy określone przez dokument Polityki Bezpieczeństwa Informacji mają zastosowanie, w szczególności do:

1. wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych, w których przetwarzane są informacje podlegające ochronie,
2. informacji będących własnością Zespołu Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz;
3. wszystkich lokalizacji Zespołu Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz, czyli budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.

Zasady działania, kompetencje i zakresy odpowiedzialności opisane w dokumentach Polityki Bezpieczeństwa Informacji oraz dokumentach powiązanych obowiązują wszystkich pracowników w rozumieniu w szczególności ustawy o organizowaniu i prowadzeniu działalności społecznej oraz przepisów Kodeksu Pracy, a także innych osób mających dostęp do chronionych informacji (np. praktykantów, stażystów, pracowników firm zewnętrznych realizujących prace w Zespole Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz. Dokument ma zastosowanie do wszystkich informacji chronionych niezależnie od formy, w jakiej są przechowywane (papierowej, elektronicznej i innej).

§ 4.

DEKLARACJA KIEROWNICTWA W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI

Kierownictwo Zespołu Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz aktywnie wspiera zapewnienie bezpieczeństwa informacji w całej organizacji wskazując kierunki działania oraz przyjmując odpowiedzialność w zakresie bezpieczeństwa informacji. Dyrektor ma świadomość znaczenia przetwarzanych informacji dla realizacji misji i celów Szkoły oraz jest świadomy potrzeby ochrony informacji.

Dyrektor zapewnia środki niezbędne do realizacji Polityki Bezpieczeństwa Informacji. Szczegółowe rozwinięcie zagadnień objętych Deklaracją jest udokumentowane w Polityce Bezpieczeństwa Informacji, kierunkowych politykach oraz innych aktach wewnętrznych Zespołu Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz.

W Szkole zapewnia się bezpieczeństwo informacji poprzez:

a) zarządzanie ryzykiem,
b) zarządzanie zmianami,
c) zarządzanie ciągłością działania organizacji,
d) zarządzanie incydentami.

§ 5.

ORGANIZACJA BEZPIECZEŃSTWA INFORMACJI

Struktura zarządzania bezpieczeństwem informacji przedstawia się następująco:

Dyrektor Zespołu Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz jest odpowiedzialny za zapewnienie zasobów niezbędnych dla funkcjonowania, utrzymania i doskonalenia bezpieczeństwa informacji oraz poszczególnych zabezpieczeń.

Inspektor Ochrony Danych (dalej: IOD), do którego zadań w szczególności należy koordynacja procesów związanych z bezpieczeństwem informacji oraz zapewnienie przestrzegania przepisów o ochronie danych osobowych.

Wszyscy pracownicy są odpowiedzialni za bezpieczeństwo informacji w Zespołu Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz zgodnie z posiadanymi zakresami obowiązków, zawartymi umowami oraz innymi dokumentami obowiązującymi w jednostce, zwłaszcza Polityką Bezpieczeństwa Informacji i politykami szczegółowymi. Każdy pracownik jak i stażyści czy praktykanci są zapoznawani z zasadami bezpieczeństwa oraz z aktualnymi politykami ochrony informacji w Zespole Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz.

W umowach ze stronami trzecimi zawierane są postanowienia dotyczące obowiązku zachowania poufności i nieujawniania informacji. Dodatkowo strona zewnętrzna składa

oświadczenie odnośnie do świadomości swoich zobowiązań w zakresie przetwarzania i zarządzania informacjami należącymi do Zespołu Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz.

§ 6.
ZASADY ZARZĄDZANIA INFORMACJĄ

Poniżej prezentowane zasady są podstawą realizacji Polityki Bezpieczeństwa Informacji:

1. **zasada uprawnionego dostępu** – każdy pracownik przechodzi szkolenie z zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji i podpisuje stosowne oświadczenie o zachowaniu poufności,
2. **zasada przywilejów koniecznych** – każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań,
3. **zasada wiedzy koniecznej** – każdy pracownik posiada wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań,
4. **zasada usług koniecznych** – zgodne tylko ze swoim statutowym zakresem działania,
5. **zasada świadomości zbiorowej** – wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych i aktywnie uczestniczą w tym procesie,
6. **zasada indywidualnej odpowiedzialności** – za bezpieczeństwo poszczególnych elementów odpowiadają konkretne osoby,
7. **zasada kompletności** – skuteczne zabezpieczenie jest tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania informacji,
8. **zasada ewolucji** – każdy system musi ciągle dostosowywać mechanizmy wewnętrzne do zmieniających się warunków zewnętrznych,
9. **zasada zamkniętego pomieszczenia** – ostatnia osoba wychodząca z pomieszczenia na zakończenie dnia pracy, jest zobowiązana zamknąć drzwi na klucz. Niedopuszczalne jest pozostawienie otwartych pomieszczeń w godzinach pracy, gdy nikogo upoważnionego nie ma w środku,

10. **zasada nadzorowanych dokumentów** – po godzinach pracy w zamkniętych szafach lub biurkach należy przechowywać wszystkie dokumenty, którym zgodnie z klasyfikacją informacji Zespołu Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz zostały uznane za informacje chronione,

11. **zasada czystego biurka** – należy unikać pozostawiania dokumentów na biurku bez opieki. Po zakończeniu pracy należy uprzątnąć biurko z dokumentów papierowych lub innych nośników danych,
12. **zasada czystego ekranu** – każdy komputer musi mieć ustawiony wygaszacz ekranu zabezpieczający hasłem. Wygaszacz powinien włączać się automatycznie po 5 minutach bezczynności użytkownika. Użytkownicy przed pozostawieniem włączonego komputera bez opieki, zobowiązani są zablokować komputer lub w przypadku dłuższej nieobecności wylogować się z systemu. Po zakończonym dniu, komputer należy wyłączyć,
13. **zasada czystych drukarek** – informacje chronione w Zespole Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz należy zabierać z drukarek natychmiast po wydrukowaniu. W przypadku nieudanej próby wydrukowania, użytkownik zobowiązany jest skontaktować się z osobą odpowiedzialną za dane urządzenie lub zgłosić incydent bezpieczeństwa,
14. **zasada czystego kosza** – dokumenty papierowe z wyjątkiem materiałów promocyjnych, marketingowych i informacyjnych należy niszczyć w sposób uniemożliwiający ich odczytanie *(w niszczarce)*. Niszczenie takich dokumentów powinno odbywać się na bieżąco.

§ 7.

UTRZYMANIE ODPOWIEDNIEGO POZIOMU BEZPIECZEŃSTWA INFORMACJI

Niezbędną praktyką po wdrożeniu mechanizmów ochrony informacji jest monitorowanie zagrożeń i zabezpieczeń, systematyczna weryfikacja i aktualizacja dokumentów Polityki Bezpieczeństwa Informacji i stosowanych zabezpieczeń. Nakłady ponoszone na zabezpieczenie muszą być poprzedzone analizą ryzyka i kosztów, adekwatnie do potencjalnych strat spowodowanych naruszeniem bezpieczeństwa. Zadaniem Polityki Bezpieczeństwa Informacji jest zmniejszenie ryzyka płynącego z zagrożeń do akceptowalnego poziomu, to znaczy:

a) zapobieganie przypadkom naruszenia bezpieczeństwa zasobów informacyjnych,
b) zminimalizowanie możliwości takiego naruszenia bezpieczeństwa,
c) umożliwienie wczesnego jego wykrycia,
d) zminimalizowanie strat związanych z takim naruszeniem oraz sprawne usunięcie jego skutków.

W Zespole Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz zarządzenie ryzykiem w bezpieczeństwie informacji realizowane jest zgodnie z Polityką Zarządzania Ryzykiem, która stanowi załącznik nr 8 do niniejszej Polityki. Określa szczegółowo:

- sposoby identyfikacji ryzyka,
- ocenę ryzyka,
- analizę istotności ryzyka,
- metody reakcji na ryzyko,
- zasady dokumentowania analizy ryzyka.

§ 8
DOKUMENTACJA BEZPIECZEŃSTWA INFORMACJI

Dokumentacja składa się z Polityki Bezpieczeństwa Informacji oraz polityk szczegółowych. Niniejszy dokument jest dokumentem nadrzędnym w stosunku do wszystkich polityk, aktów wewnętrznych regulujących obszar bezpieczeństwa informacji w Zespole Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz.

Dokumentacja obejmuje m.in. Politykę Bezpieczeństwa Informacji, polityki uszczegółowiające zasady postępowania:

1. Polityka ochrony danych osobowych w Szkole – zał. Nr 1.
2. Polityka Zarządzania Infrastrukturą Techniczną – zał. Nr 2.
3. Polityka Kontroli Dostępu do Informacji– zał. Nr 3.
4. Polityka Tworzenia Kopii Zapasowych – zał. Nr 4.
5. Polityka Klasyfikacji Informacji – zał. Nr 5.
6. Polityka Postępowania z Incydentami oraz w sytuacji naruszenia ochrony danych osobowych – zał. Nr 6.
7. Polityka Profilaktyki Antywirusowej – zał. Nr 7.
8. Polityka Zarządzania Ryzykiem i Ocena Skutków dla przetwarzania danych żął. Nr 8.,

oraz dokumentację powiązaną, wprowadzoną odrębnymi zarządzeniami Zespołu Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz, a w szczególności:

1. Instrukcja gospodarowania kluczami w Szkole.

§ 9.
ODPOWIEDZIALNOŚĆ ZA OCHRONĘ INFORMACJI

Skuteczna ochrona zasobów informacyjnych Szkoły, wspólnego działania i zaangażowania wszystkich pracowników. Zarówno dyrektor, jak i wszyscy pracownicy są zobowiązani odpowiednio do swoich obowiązków i zajmowanych stanowisk, do przestrzegania Polityki

Bezpieczeństwa Informacji, a zwłaszcza zasad zawartych w procedurach, instrukcjach i innych dokumentach Polityki. Pracownicy w szczególności zobowiązani są do przestrzegania procedur opisujących zasady korzystania z haseł, procedur ochrony antywirusowej oraz procedur eksploatacji systemów informatycznych, a także do przestrzegania zakazu udostępniania hasła do swojego komputera, zakazu korzystania z nielegalnego oprogramowania oraz zakazu instalowania jakiegokolwiek oprogramowania bez zgody dyrektora. Pracownicy są zobowiązani do używania zasobów informacyjnych Zespołu Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz.

W przypadku osób, z którymi jednostka zawiera umowy cywilno-prawne, z których wynika, że będą korzystali z zasobów informacyjnych, należy w zawieranej umowie wprowadzić klauzulę dotyczącą obowiązku przestrzegania postanowień Polityki Bezpieczeństwa Informacji.

Polityka Bezpieczeństwa Informacji obowiązuje wszystkich dostawców usług i oprogramowania, jednostki zewnętrzne i ich pracowników, o ile w trakcie realizacji umowy otrzymują dostęp do zasobów informatycznych Szkoły. W tym przypadku należy w zawieranej umowie wprowadzić klauzulę dotyczącą obowiązku przestrzegania postanowień Polityki Bezpieczeństwa Informacji oraz klauzulę o możliwości przeprowadzenia audytu bezpieczeństwa informacji w jednostce zewnętrznej. Dostęp do zasobów informatycznych i pomieszczeń uzyskują po wcześniejszym otrzymaniu stosownego upoważnienia i zapoznaniu się z Polityką Bezpieczeństwa Informacji. Dostęp do zasobów jest ograniczony do okresu zdefiniowanego w umowie.

Odpowiedzialność za bezpieczeństwo informacji Szkoły obejmuje nie tylko siedzibę, ale także wszelkie sytuacje, w których informacje związane z działalnością są przetwarzane poza jego siedzibą. Obejmuje to w szczególności zdalny dostęp do sieci komputerowej.

§ 10. SANKCJE ZA NARUSZENIE ZASAD BEZPIECZEŃSTWA INFORMACJI

Nieprzestrzegania zasad zawartych w dokumentach Polityki Bezpieczeństwa Informacji Zespołu Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz, jest naruszeniem obowiązków pracowniczych wynikających w szczególności z ustaw o pomocy społecznej oraz Kodeksu Pracy i może pociągnąć za sobą skutki dyscyplinarne oraz spowodować pociągnięcie do odpowiedzialności wynikającej z przepisów prawa. Naruszenie zasad ochrony informacji może spowodować pociągnięcie do odpowiedzialności karnej wynikającej z przepisów:

1) Ustawy o ochronie danych osobowych,
2) Kodeksu Karnego dotyczącego przestępstw przeciwko ochronie informacji,
3) Przepisów chroniących tajemnice zawodowe.

§ 11.

ZASADY ROZPOWSZECHNIANIA DOKUMENTU ORAZ TRYB WPROWADZANIA ZMIAN

Do zapoznania się z Polityką Bezpieczeństwa Informacji Zespołu Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz i dokumentacją powiązaną zobligowani są wszyscy pracownicy. Niniejszy dokument powinien być udostępniany uprawnionym podmiotom zewnętrznym w celu zapoznania się i postępowania w zgodzie z postanowieniami niniejszego dokumentu.

Stanowisko ds. kadr przekazuje do zapoznania się nowo zatrudnionym pracownikom oraz stażystom i praktykantom Politykę Bezpieczeństwa Informacji wraz z dokumentami związanymi. Nowo zatrudniony pracownik, stażysta lub praktykant jest zobowiązany zapoznać się i złożyć pisemne oświadczenie potwierdzające znajomość zasad, reguł i postanowień zawartych w ww. dokumentach.

Dokumentacja Polityki Bezpieczeństwa Informacji podlega przeglądowi i weryfikacji:

1) na polecenie dyrektora,
2) w przypadku wystąpienia poważnych incydentów związanych z bezpieczeństwem informacji,
3) w celu realizacji zaleceń wynikających z przeprowadzonych audytów lub kontroli,
4) w przypadku wejścia w życie nowych przepisów dotyczących bezpieczeństwa informacji,
5) w przypadku poważnych modyfikacji infrastruktury teleinformatycznej,
6) w przypadku zawarcia umów, z których wynikają zobowiązania związane z bezpieczeństwem informacji,
7) okresowo **nie rzadziej niż raz** w roku.

Zmiany w dokumentach wprowadza IOD, które zatwierdza dyrektor i wprowadza w drodze zarządzenia.

POLITYKA KALSYFIKACJI INFORMACJI

1. Wprowadzenie

Zespół Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz zarządza swoimi aktywami informacyjnymi poprzez zapewnienie im wymaganego poziomu bezpieczeństwa. Identyfikowane są aktywa informacyjne i klasyfikowane zgodnie ze stawianymi im wymaganiami w zakresie ochrony.

Klasyfikacja informacji jest spojrzeniem na organizację przez pryzmat przetwarzanych danych. Klasyfikacja informacji jest czynnością grupowania wzajemnie powiązanych informacji, określania znaczenia tych grup dla jednostki oraz przypisywania ujednoliconych etykiet ułatwiających gromadzenie, odszukiwanie i analizę informacji. Celem klasyfikacji jest zapewnienie przypisania informacjom odpowiedniego poziomu ochrony zgodnego z ich wagą dla Zespołu Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz oraz określenie, które informacje są ważne i należy je chronić, a które nie posiadają wartości prawnej i nie muszą podlegać ochronie.

Klasyfikacja uwzględnia wymagania prawne, które zostały określone przede wszystkim w następujących aktach prawnych:

- ustawie o ochronie danych osobowych,
- ustawie o dostępie do informacji publicznej,
- ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne,
- w ustawie o prawach autorskich i prawach pokrewnych.

Klasyfikacja została wprowadzona w celu uporządkowania w Zespole Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz postępowania z informacją. Informacje są głównym zasobem informacyjnym Szkoły, w związku z czym został uregulowany sposób postępowania z informacjami, w szczególności tymi, których ujawnienie może narazić Szkołę na szkodę.

Podstawowym elementem klasyfikacji są grupy informacji. Do określenia poziomu bezpieczeństwa danej grupy informacji przyjęto takie atrybuty jak **poufność, integralność oraz dostępność**, wymagane w Zespole Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz.

Przez **poufność** rozumie się zapewnienie, że dostęp do informacji mają wyłącznie osoby uprawnione.
Przez **integralność** rozumie się zapewnienie, iż informacje nie zostały zmienione lub zniszczone w nieautoryzowany sposób

Przez **dostępność** rozumie się zapewnienie, iż informacje będą udostępniane z zasobów o różnym poziomie bezpieczeństwa z uwagi na miejsce i sposób przechowywania.

Polityka Kwalifikowania Informacji określa dwie grupy kwalifikacyjne:

1. informacje ogólnodostępne *(publiczne),*
2. informacje do użytku wewnętrznego wraz z przepisami o ochronie danych osobowych,

2. Sposób postępowania z informacjami z różnych klas:

	Informacje ogólnodostępne (publiczne)	**Informacje do użytku wewnętrznego wraz z przepisami o ochronie danych osobowych**
Przykłady:	Np. zaproszenia, oferty szkoleniowe, reklamy, publikacje itp.	Dokumenty zawierające dane osobowe, akta spraw, protokoły, umowy z podmiotami publicznymi itp.
DLA DOKUMENTÓW PAPIEROWYCH:		
Rozpowszechnianie i udostępnianie informacji	Dopuszczalne	1. Rodzicom: w przypadku wykazani, że są strony w sprawie (na wniosek), 2.Współpracownikom: osobom biorącym udział w danym postępowaniu administracyjnym, 3. Innym osobom: niedozwolone udostępnienie informacji, Dopuszczalne umowy z podmiotami zewnętrznymi z wyłączeniem informacji stanowiących tajemnicę przedsiębiorstwa, która oznacza wszelkie informacje, których ujawnienie przyniosło lub mogłoby przynieść uszczerbek dla interesów przedsiębiorstwa

Oznaczanie dokumentów papierowych	Brak oznaczeń	Zgodnie z instrukcją kancelaryjną

Przechowywanie	W sposób zapewniający ochronę przed zniszczeniem	Przechowywanie w zamykanych szafach, w sposób zapewniający ochronę przed zniszczeniem lub dostępem osób niepowołanych
Kopiowanie – kserowanie	Dopuszczalne	Dopuszczalne. Należy pamiętać o zabraniu oryginału kopii z kserokopiarki. Należy pamiętać o numeracji kopii.
Niszczenie	Wyrzucenie do segregowanych śmieci papierowych. Nie ma potrzeby używania niszczarki	Niszczenie w niszczarce
Przesyłanie faxem	Dopuszczalne	Dopuszczalne. Należy się upewnić, że wybrano poprawny numer. Jeżeli istnieje możliwość odbioru przez osobę niepowołaną, to należy wybrać inny sposób przekazania.
Przesyłanie pocztą, kurierem	Dopuszczalne	Dopuszczalne. Należy popranie zaadresować kopertę- z dokładnym określeniem osoby, która ma ją odebrać
PRZEKAZY AUDIOWIZUALNE		
Przekazywanie drogą telefoniczną – przez numery wewnętrzne	Dopuszczalne	Dopuszczalne. Przekazanie informacji tylko po określeniu tożsamości rozmówcy. Należy się upewnić, że żadna osoba nieuprawniona nie usłyszy naszej rozmowy.
Przekazywanie drogą telefoniczną – przez telefony stacjonarne, komórkowe	Dopuszczalne	Niedopuszczalne
Przekazywanie w trakcie wideokonferencji	Dopuszczalne	Nie występuje
DLA INFORMACJI ELEKTRONICZNYCH		
Oznaczenie dokumentów	Brak	Zgodne z JRWA.

Przechowywanie w formie plików/baz/aplikacji	Dopuszczalne w każdej formie	Pliki należy przechowywać w osobnych katalogach, do których prawo dostępu mają upoważnione osoby. W aplikacjach dostęp do danych osobowych jest możliwy tylko w przypadku, gdy użytkownik poda swój identyfikator i hasło i zostanie pozytywnie uwierzytelnione oraz posiada prawo dostępu do powyższych danych.
Udostępnianie na stronach intranet i stronach instytucji	Dopuszczalne	Niedopuszczalne

Przechowywanie na komputerach przenośnych	Dopuszczalne	Dopuszczalne, w razie potrzeby przeniesienia dokumentacji wymagane jest zabezpieczenie komputera hasłem. Za bezpieczeństwo danych umieszczonych na komputerze przenośnym odpowiada właściciel komputera.
Przechowywanie w elektronicznych kalendarzach, organizerach (Outlook, Google Calendar itp.)	Dopuszczalne	Niedopuszczalne
Ochrona informacji znajdujących się na ekranie	Nie ma potrzeby	Monitory, na których są wyświetlane informacje muszą być ustawione tak, aby osoby nieupoważnione nie mogły zobaczyć zawartości ekranu. Dodatkowo trzeba ustawić tak monitor, żeby ekran nie był zwrócony bezpośrednio w stronę okien. W przypadku dłuższej nieobecności: blokowanie komputera lub wygaszacze ekranu.
Przechowywanie na pendrive'ach, dyskach przenośnych, kartach pamięci	Dopuszczalne	Pliki z informacjami nie powinny być przechowywane na nośnikach zewnętrznych, natomiast jeżeli zachodzi taka konieczność, to należy je przenosić w formie zaszyfrowanej.
Przechowywanie na nośnikach	Dopuszczalne	Dane osobowe należy przechowywać na nośnikach w formie zaszyfrowanej. Nośniki należy przechowywać w zamykanych szafach.
Kasowanie	Kasowanie informacji z dysków twardych może się odbywać poprzez wykonanie standardowej opcji usuwania	Kasowanie informacji z dysków twardych może się odbywać poprzez wykonanie standardowej opcji usuwania.

Drukowanie	Dopuszczalne	Informacje należy drukować tak, aby wydruk nie mógł zostać przejęty przez osoby nieupoważnione.
Przesyłanie pocztą elektroniczną, komunikatorami internetowymi itp.	Dopuszczalne	Dopuszczalne. Informacje można przesłać pocztą elektroniczną przy zastosowaniu protokołu SSL.
Sposób postępowania z informacjami i sprzętem w trakcie podróży	Nie ma potrzeby szczególnej ochrony informacji	W trakcie podróży nośniki/wydruki/sprzęt z danymi osobowymi należy trzymać cały czas przy sobie: nie można zostawiać w samochodzie, nie należy traktować jako bagaż podręczny, nie należy zostawiać w szafkach, skrytkach lub pokojach hotelowych.

ZASOBY LUDZKIE:		
Rozmowy na dany temat w siedzibie instytucji	Dopuszczalne	Dopuszczalne. Można rozmawiać z osobą upoważnioną. Należy uważać, czy rozmowa nie może być podsłuchana przez osobę postronną.
Rozmowy na dany temat w miejscach publicznych	Dopuszczalne	Zakaz rozmów z kimkolwiek.
Rozmowy na dany temat w domu	Dopuszczalne	Zakaz rozmów z kimkolwiek.
Rozmowy na dany temat w trakcie podróży	Dopuszczalne	Zakaz rozmów z kimkolwiek.

POLITYKA KONTROLI DOSTĘPU DO INFORMACJI

1. Definicja pojęć stosowanych w Polityce:

Stanowisko – pojedynczy komputer osobisty lub terminal przeznaczony do określonych zadań związanych między innymi z dostępem do sieci komputerowej Szkoły.

Zasoby informatyczne – ogół systemów informatycznych wykorzystywanych przez daną organizację.

Spam – niechciane wiadomości elektroniczne. Najbardziej rozpowszechniony jest spam wysyłany za pośrednictwem poczty elektronicznej. Zwykle (choć nie zawsze) jest wysyłany masowo. Istotą spamu jest rozsyłanie dużej liczby informacji komercyjnych o jednakowej treści do nieznanych sobie osób.

Konto – to zbiór zasobów i uprawnień mający unikalny identyfikator w systemie informatycznym lub sieci komputerowej.

Użytkownik – to osoba korzystająca z systemu komputerowego. Użytkownicy mogą być identyfikowani w celach zliczenia czasu pracy, bezpieczeństwa, czy też zarządzania zasobami. Aby użytkownik został zidentyfikowany, użytkownik posiada konto (konto użytkownika) i hasło (lub inny sposób autentykacji – np. informacje biometryczne). Użytkownicy uzyskują dostęp do systemów przez interfejs użytkownika, a sam proces identyfikacji jest nazywany logowaniem.

2. Cel polityki

Celem wdrożonej w Szkole polityki kontroli dostępu do informacji jest zapewnienie właściwego poziomu dostępu do systemów informatycznych przez użytkowników oraz uniemożliwienie dostępu osobom niepowołanym. Procedura określa zasady tworzenia i przydzielania kont oraz haseł dostępu do systemów informatycznych.

Szkoła wykorzystuje kontrolę dostępu i inne środki bezpieczeństwa, aby zapewnić poufność, integralność i dostępność informacji przy pomocy jego systemów komunikacyjnych i komputerowych.

3. Zarządzanie dostępem użytkowników

Nadawanie uprawnień do korzystania z systemu informatycznego opiera się o zasadę wiedzy uzasadnionej i zasadę minimalnych uprawnień. Użytkownik może mieć dostęp tylko do tych informacji, które są mu potrzebne do realizacji zadań- dostęp do innych danych jest zabroniony. Dla każdego rodzaju użytkownika tworzona **jest rola**, opisująca jego uprawnienia do korzystania z systemu informatycznego.

Przyznawanie dostępu do wszystkich systemów i usług informacyjnych w przedszkolu opiera się na formalnej procedurze rejestrowania i wyrejestrowywania użytkowników. Dostęp do konkretnego systemu informatycznego nadaje ADO lub osoba przez niego upoważniona określając identyfikację systemu, identyfikację osoby, poziom uprawnień (rolę), cel uzyskania uprawnień. Każdemu użytkownikowi nadaje się identyfikator i hasło dostępu. Identyfikator składa się z elementów zawierających imię i nazwisko użytkownika. Należy zapewnić unikatowość pierwszego hasła, które powinno być niezwłocznie zmienione przez użytkownika na inne, znane tylko sobie. Każde hasło powinno spełniać następujące wymagania:

- minimalna długość hasła powinna wynosić 8 znaków,
- hasło powinno zawierać małe i duże litery, cyfry oraz znaki specjalne,
- hasło nie może być takie samo jak identyfikator,
- hasło nie może się składać z następujących elementów: imienia, nazwiska, numerów telefonów, adresów, numerów PIN, poprzednich haseł,
- hasło musi być zmieniane przez użytkownika nie rzadziej niż co 30 dni.

W razie zapomnienia hasła przez użytkownika nowe hasło jest ustanawiane przez ADO lub osobę przez niego upoważnioną, a następnie jest **wymuszana zmiana** hasła przez użytkownika. Hasło dostępu zapisywane są na ekranie monitora w formie niejawnej i mogą być znane tylko użytkownikowi.

Użytkownicy powinni być świadomi reguł używania haseł oraz powinni zobowiązać się do nieujawniania ich. Zabronione jest przechowywanie haseł w formie jawnej w systemach informatycznych.

W przypadku wdrożenia instalacji systemów informatycznych **bezwzględnie należy zmienić** hasło dostarczone/ustalone przez producenta oprogramowania.

Ww. procedurą obejmuje się postępowanie o nadanie, zmianę lub cofnięcie uprawnień w przypadku **dostępu do poczty elektronicznej, lokalnego systemu operacyjnego Windows, panelu administracyjnego Biuletynu Informacji Publicznej, VPN oraz wszystkich pozostałych systemów informatycznych zarówno zawierających jak i niezawierających danych osobowych oraz w stosunku do kont uprzywilejowanych.**

W przypadku zakończenia stosunku pracy, umowy lub porozumienia z użytkownikiem lub zmiany jego zakresu stanowiska pracy ADO zapewnia niezwłoczne usunięcie lub blokadę przydzielony użytkownikowi identyfikator.

Dostęp do informacji przechowywanych i przetwarzanych w Szkole jest poddany kontroli.

Kontrola polega na:

1. wydzieleniu obszarów przeznaczonych do przechowywania oraz przetwarzania poszczególnych zbiorów danych i zapewnieniu odpowiednich barier fizycznych przeciwdziałających nieuprawnionemu dostępowi,
2. zarządzaniu uprawnieniami poszczególnych użytkowników w sposób zapewniający dostęp wyłącznie do danych wymaganych do wykonywania obowiązków służbowych, jeśli dane te podlegają ochronie z jakiejkolwiek przyczyny. Kontroli podlega poziom przyznanego użytkownikom dostępu do systemów, programów, baz danych,
3. stosowaniu bezpiecznych systemów przetwarzania informacji,
4. nadzorowaniu działalności stron trzecich, mogących wpłynąć na bezpieczeństwo informacji,
5. bieżącym informowaniu pracowników o wszelkich zmianach w zakresie regulacji dotyczących przechowywania, przetwarzania i udostępniania informacji.

4. Zasady postępowania dotyczące pracy na odległość oraz urządzeń przenośnych i nośników danych wynoszonych poza siedzibę Szkoły.

Praca na odległość może być wykonywana wyłącznie przez pracowników posiadających umowę o odpowiedzialności materialnej za powierzone mienie.

Przy korzystaniu z urządzeń mobilnych stosuje się następujące zasady:

1) użytkownik otrzymujący komputer przenośny podpisuje umowę, w której zobowiązuje się do przestrzegania zaleceń związanych z ochroną laptopa:
    a. laptop powinien być transportowany pod kontrolą użytkownika lub innej upoważnionej osoby,
    b. laptop nie powinien być pozostawiany w sposób narażający go na kradzież,
    c. dyski na komputerach przenośnych są szyfrowane,
    d. nie zezwala się na pracę nad informacjami wrażliwymi w miejscach publicznych,
    e. użytkownicy laptopów powinni zapewnić systematyczne tworzenie kopii zapasowych,
    f. użytkownicy są zobowiązani do aktualizacji systemów operacyjnych z zachowaniem rozwiązań organizacyjnych wskazanych przez ADO,
2) zabrania się kopiowania i przechowywania danych stanowiących własność Szkoły na smartfonach,
3) zabrania się korzystania z prywatnych laptopów i innych urządzeń przenośnych do kopiowania i przetwarzania danych należących do Szkoły,
4) zobowiązuje się przy korzystaniu z urządzeń mobilnych do korzystania wyłącznie z bezpiecznych sieci.

Pracownicy użytkujący przenośnie komputery, w których przetwarzane są dane osobowe, zobowiązani są zachować szczególną ostrożność podczas transportu i przechowywania tego

komputera. W celu zabezpieczenia ingerencji osób niepowołanych, dostęp do komputera musi być zabezpieczony hasłem i zabronione jest użytkowanie komputera osobom nieupoważnionym. Komputera przenośnego nie należy pozostawiać w miejscu, w którym może wystąpić niebezpieczeństwo utraty lub wycieku danych.

5. Kontrola dostępu do sieci komputerowej

Użytkownicy powinni mieć bezpośredni dostęp tylko do zasobów określonych dla nich przeznaczonych.

6. Zabezpieczanie systemu operacyjnego

W celu zabezpieczenia systemu informatycznego przed działaniem niebezpiecznego oprogramowania zabrania się:

1) pobierania, instalowania i uruchamiania jakiegokolwiek oprogramowania, które nie zostało zatwierdzone do użytku w Szkole;
2) korzystania z nośników przenośnych innych niż zatwierdzone do użytku w Szkole;
3) używania służbowych nośników przenośnych do celów prywatnych oraz w niezarejestrowanych stacjach roboczych;
4) otwierania poczty elektronicznej, której tytuł nie sugeruje związku z pełnionymi obowiązkami służbowymi; w przypadkach wątpliwych należy skonsultować się z IOD lub ADO;
5) korzystania z Internetu w celach nie związanych z pełnionymi obowiązkami służbowymi;
6) podłączania komputerów do sieci zewnętrznych za pośrednictwem modemów lub innych urządzeń dostępowych.

Potencjalnymi źródłami przedostania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są:

1) załączniki do poczty elektronicznej,
2) przeglądane strony internetowe,
3) pliki i aplikacje pochodzące z prywatnych nośników wymiennych uruchamiane i odczytywane na stacji roboczej.

System informatyczny jest zabezpieczony przed działaniem niebezpiecznego oprogramowania poprzez:

1) oprogramowanie antywirusowe,
2) zaporę sieciową,
3) aktualizację oprogramowania systemowego,

4) konfigurację oprogramowania minimalizującą ryzyko naruszenia bezpieczeństwa.

Każdy pracownik przetwarzający dane osobowe przy użyciu komputera w wypadku jakichkolwiek podejrzeń dotyczących obniżenia bezpieczeństwa danych osobowych, powinien poinformować o tym fakcie ADO oraz IOD w Szkole.

7. Odpowiedzialność

Za wdrożenie polityki kontroli dostępu w zakresie bezpieczeństwa systemów IT oraz bezpieczeństwo fizyczne odpowiedzialność ponosi ADO.

Użytkownik rozpoczynający pracę w systemie zobowiązany jest przestrzegać procedur, które mają na celu sprawdzenie zabezpieczenia pomieszczenia, w którym przetwarzane są dane osobowe, swojego stanowiska pracy oraz stanu sprzętu komputerowego a w szczególności:

1. przed wejściem do pomieszczenia sprawdzić czy na drzwiach i zamkach nie ma widocznych śladów prób niepowołanego ich otwierania,
2. sprawdzić stan okien oraz ocenić czy w pomieszczeniu nie ma znaków wskazujących na pobyt w nim osób nieuprawnionych,
3. sprawdzić stan sprzętu informatycznego oraz zamknięcie szaf i biurek,
4. po włączeniu komputera ocenić jakość jego pracy i stwierdzić zmiany.

Użytkownik przed przystąpieniem do przetwarzania informacji powinien zalogować się w systemie, posługując się swoim identyfikatorem i hasłem.

Każdy użytkownik jest zobowiązany do ochrony swojego hasła, nieujawniania go, niezapisywania na papierze bądź innym nośniku, jeśli ten zapis nie może być przechowywany w sposób bezpieczny. Użytkownicy zostali zobowiązani do dobierania haseł w taki sposób, żeby były trudne do odgadnięcia, zmiany haseł zgodnie z zaleceniami Polityki Bezpieczeństwa Informacji. W przypadku podejrzenia złamania hasła użytkownik jest zobowiązany zmienić je na nowe, a o swoich podejrzeniach poinformować ADO lub IOD.

Użytkownik ponosi odpowiedzialność za czynności wykonywane w systemie przy użyciu identyfikatora i hasła, którymi się posługuje lub posługiwał. Użytkownik zobowiązany jest do utrzymania haseł dostępu w tajemnicy, a w szczególności do dołożenia starań, w celu uniemożliwienia zapoznania się z nimi osób trzecich, nawet po ustaniu ich ważności.

Użytkownik w czasie pracy powinien stosować przedsięwzięcia zapewniające bezpieczeństwo informacji:

1. ustawić ekrany monitorów w pomieszczeniach tak, aby uniemożliwić podgląd osób nieuprawnionych,
2. dopilnować, aby w pomieszczeniach stanowiących obszar przetwarzania danych osobowych przebywały osoby trzecie, tylko w obecności uprawnionych,

3. stosować wygaszacze ekranów, które włączają się po upływie 5 minutach bezczynności komputera – wygaszacze ekranów zabezpiecza się hasłami,
4. wylogować się z systemu w przypadku, kiedy przerwa w pracy trwa dłużej niż 60 minut.

Po zakończeniu pracy użytkownik powinien przestrzegać następujących zasad:

1. wylogować się z systemu,
2. sprawdzić czy nie zostały pozostawione bez nadzoru elektroniczne nośniki informacji,
3. upewnić się, że szafy i biurka z dokumentacją są zamknięte,
4. wyłączyć odbiorniki energii elektrycznej, zamknąć pomieszczenie.

Pracownicy są uświadamiani o swojej odpowiedzialności za powierzony sprzęt. Użytkownik przerywając pracę z systemem powinien wylogować się lub w przypadku planowanej krótkiej nieobecności zabezpieczyć dostęp do komputera hasłem. Wychodząc z pokoju, w którym znajdują się komputery, powinien zamknąć drzwi na klucz.

Załącznik Nr 1
do Polityki Bezpieczeństwa Informacji w Zespole Szkół
w Bystrzejowicach Pierwszych im. Heleny Babisz

POLITYKA OCHRONY DANYCH OSOBOWYCH W ZESPOLE SZKÓŁ W BYSTRZEJOWICACH PIERWSZYCH IM. HELENY BABISZ

§ 1.
Postanowienia ogólne

1. **Polityka ochrony danych osobowych w Zespole Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz** zwana dalej *Polityką ochrony danych* jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora danych osobowych w celu spełnienia wymagań zawartych w Rozporządzeniu 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 ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. , poz. 1781).

2. **Polityka ochrony danych** stanowi jeden ze środków organizacyjnych mających na celu wykazanie, że przetwarzanie danych osobowych w Szkole odbywa się zgodnie z powyższym rozporządzeniem.

§ 2.
Definicje

Określenia i skróty użyte w Polityce Bezpieczeństwa oznaczają:

1) **RODO -** 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);
2) **Ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r., poz. 1781);
3) **Podmiot przetwarzający –** to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek innych organ przetwarzający dane osobowe w imieniu administratora;
4) **Zbiór danych osobowych** - oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
5) **Dane osobowe** - oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio

zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczna, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

6) **Przetwarzanie danych -** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

7) **Zgoda osoby, której te dane dotyczą** - oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

§ 3.

Obszary przetwarzania danych osobowych

1. Obszar przetwarzania danych osobowych w Szkole obejmuje budynki, pomieszczenia i części pomieszczeń, w których przetwarzane są dane osobowe, tzw. miejsca, w których wykonuje się operacje na danych osobowych (wpisuje, zmienia, kopiuje, przechowuje itp.) oraz miejsca, gdzie przechowuje się nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające elektroniczne nośniki informacji, pomieszczenia, w których składowane są uszkodzone nośniki danych).

2. Obszar przetwarzania danych osobowych określony jest w „Wykazie budynków i pomieszczeń tworzących obszar, w których przetwarzane są dane osobowe”, stanowiącym **załącznik nr 1** do Polityki ochrony danych.

3. Wykaz ten zawiera następujące informacje:

1) wykaz budynków, zawierający ich adresy,

2) wykaz pomieszczeń, zawierający:

a) numer pomieszczenia i jego przeznaczenie,

b) lokalizację pomieszczenia,

c) wskazanie liczby osób pracujących w pomieszczeniu: wskazanie stanowisk i liczby osób,

d) określenie zabezpieczenia pomieszczenia.

4. Warunki ochrony przetwarzania danych tego obszaru określone zostały w **załączniku nr 2** do Polityki „Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe”.

§ 4.
Rejestr czynności przetwarzania

1. ADO prowadzi rejestr czynności przetwarzania danych osobowych do wszystkich prowadzonych procesów przetwarzania danych osobowych w szkole. Rejestr czynności przetwarzania danych w Szkole określony został w **załączniku nr 3** do Polityki ochrony danych – *„Rejestr czynności przetwarzania danych osobowych*". Rejestr ten zawiera następujące informacje:

1) imię i nazwisko oraz dane kontaktowe administratora oraz inspektora ochrony danych;
2) cele przetwarzania;
3) kategorie osób, których dane dotyczą, oraz kategorie danych osobowych;
4) podstawa prawna;
5) źródło danych;
6) planowany termin usunięcia kategorii danych (jeżeli jest to możliwe);
7) nazwa współadministratora i dane kontaktowe (jeśli dotyczy);
8) nazwa podmiotu przetwarzającego i dane kontaktowe (jeśli dotyczy);
9) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione (innych niż podmiot przetwarzający);
10) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1;
11) DPIA (jeśli tak, lokalizacja raportu);
12) transfer do kraju trzeciego lub organizacji międzynarodowej.

2. Za prowadzenie i aktualizacje rejestru w formie pisemnej oraz w formie elektronicznej, o którym mowa w ust. 1 odpowiedzialny jest Inspektor Ochrony Danych.

§ 5.
Analiza ryzyka

1. Mając na względzie wypełnienie podstawowego obowiązku, który spoczywa na Administratorze Danych Osobowych, wynikający z Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r., zgodnie z art. 35 w Szkole dokonuje się Analizy Ryzyka dla procesów przetwarzania danych osobowych według opracowanych norm.

2. Rozporządzenie ogólne o ochronie danych pozostawia Administratorowi wybór w zakresie zastosowania konkretnej metody szacowania ryzyka.

3. Administrator w jednostce decyduje się na wykorzystanie metody szacowania ryzyka w oparciu o metodę jakościową - wielkość zagrożenia ocenia się przez pryzmat doświadczenia oraz intuicji osoby szacującej ryzyko (subiektywne odczucie).

4. Procedura prowadzenia analizy ryzyka stanowi **załącznik nr 8** do *Polityki bezpieczeństwa informacji w Szkole.*

§ 6.

Ocena skutków dla ochrony danych

1. Ocenę skutków dla ochrony danych przeprowadza się wtedy, gdy istnieje wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą.

2. Zgodnie z art. 35 RODO, jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowania operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

3. Do oceny skutków dla ochrony danych w Szkole należy stosować taki sam schemat postępowania, jak dla ogólnej analizy ryzyka, uwypuklając w poszczególnych etapach (od opisu kontekstu do postępowania z ryzykiem) te elementy, które mają istotny wpływ na skutki, jakie naruszenie ochrony danych może powodować dla osób, których dane dotyczą.

§ 7.

Administrator Danych Osobowych

1. Administratorem danych osobowych w Szkole jest Dyrektor, który ustala cele i sposoby przetwarzania danych osobowych w Szkole.

2. ADO jest odpowiedzialny za przestrzeganie i zapewnienie by dane osobowe były:

1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość);

2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami, dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami („ograniczenie celu”);

3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);
4) prawidłowe i w razie potrzeby uaktualniane, należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);
5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane, dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy RODO („ograniczenie przechowywania”);
6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).

3. ADO musi być w stanie wykazać przestrzeganie zasad określonych w ust. 2 („rozliczalność”).

4. ADO jest obowiązany wdrażać odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO oraz aby móc to wykazać.

5. ADO uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwa wystąpienia i wadze zagrożenia wynikające z przetwarzania, zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania wdraża odpowiednie środki techniczne i organizacyjne:

1) takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawo osób, których dane dotyczą,
2) aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne do osiągnięcia każdego konkretnego celu przetwarzania.

6. ADO udziela upoważnień oraz nadaje uprawnienia osobom mającym dostęp do danych osobowych.

§ 8.

Inspektor Ochrony Danych

1. Administrator Danych Osobowych wyznaczył Inspektora Ochrony Danych (IOD), do zadań którego zgodnie z treścią art. 39 RODO należy:

1) informowanie ADO, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów o ochronie danych i doradzanie im w tej sprawie;
2) monitorowanie przestrzegania RODO, innych przepisów o ochronie danych oraz polityk ADO 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;
3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
4) współpraca z Urzędem Ochrony Danych Osobowych (UODO);
5) pełnienie funkcji punktu kontaktowego dla Urzędu Ochrony Danych Osobowych (UODO) w kwestiach związanych z przetwarzaniem, w tym uprzednimi konsultacjami oraz w stosowanych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

2. Do czynności realizowanych przez Inspektora Ochrony Danych należy również śledzenie osiągnieć w dziedzinie zabezpieczania danych osobowych w ogóle i wdrażanie takich narzędzi, metod pracy oraz sposobów zabezpieczenia danych osobowych, które bezpieczeństwo to wzmocnią.

3. IOD prowadzi ewidencję wydanych przez ADO upoważnień do przetwarzania danych osobowych w Szkole;

4. IOD wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

5. IOD włączany jest we wszystkie sprawy dotyczące ochrony danych osobowych.

6. Osoby, których dane dotyczą, mogą kontaktować się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

7. IOD jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego.

8. IOD jest zobowiązany prowadzić Rejestr naruszeń bezpieczeństwa danych oraz dokumentację opisującą sposób przetwarzania danych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

9. W celu realizacji powierzonych zadań IOD w Szkole ma prawo:

1) kontrolować Użytkowników w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarzane są dane osobowe;
2) wydawać polecenia Użytkownikom Szkoły w zakresie bezpieczeństwa danych osobowych;
3) informować ADO o przypadkach naruszenia bezpieczeństwa danych osobowych;
4) żądać od wszystkich Użytkowników wyjaśnień w sytuacjach naruszenia bezpieczeństwa danych osobowych.

§ 9.

Użytkownicy systemu i użytkownicy zewnętrzni

1. W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych konieczne jest szczególne zaangażowanie ze strony każdego użytkownika systemu i użytkownika zewnętrznego w zakresie ochrony danych osobowych.

2. Użytkownicy systemu oraz użytkownicy zewnętrzni są zobowiązani do informowania o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe bezpośrednio do ADO lub IDO.

3. Użytkownicy systemu / użytkownicy zewnętrzni są zobowiązani do:

1) postępowania zgodnie z Polityką,
2) zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia,
3) ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem,
4) wykonywania niezbędnych działań w procesie przetwarzania danych celem zapewnienia właściwej ich ochrony, w tym:
    a) przestrzegania procedur związanych z otwieraniem i zamykaniem pomieszczeń, a także z wejściem do obszarów przetwarzania danych osobowych osób nieupoważnionych,
    b) informowania ADO lub IOD o podejrzanych osobach poruszających się w obszarze przetwarzania danych osobowych,
    c) dokonywania identyfikacji ewentualnych zagrożeń i przedkładanie IOD projektów i propozycji nowych rozwiązań, których celem jest zwiększenie poziomu bezpieczeństwa ochrony danych osobowych.

§ 10.

Gromadzenie danych osobowych

1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

1) osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

2) przetwarzanie jest to niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

3) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;

4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

5) przetwarzanie jest niezbędne do wykonywania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

2. Dane osobowe przetwarzane w Szkole mogą być uzyskiwane bezpośrednio od osób, których dane dotyczą lub z innych źródeł, w granicach dozwolonych przepisami prawa.

3. Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą.

4. W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.

§ 11.
Obowiązek informacyjny

W przypadku zbierania danych osobowych od osoby, której one dotyczą, podczas pozyskiwania danych osobowych należy podać jej wszystkie następujące informacje:

1) tożsamość i dane kontaktowe ADO,
2) dane kontaktowe inspektora ochrony danych;
3) cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania;
4) informacje o odbiorach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
5) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
6) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
7) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
8) jeżeli przetwarzanie odbyło się na podstawie wyrażonej zgody – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na postawie zgody przed jej cofnięciem;
9) informacje o prawie wniesienia skargi do organu nadzorczego;
10) informację czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
11) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.

2. Podanych powyżej zasad nie stosuje się, jeżeli osoba, której dane dotyczą, dysponuje już tymi informacjami.

3. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, osobie tej należy dodatkowo przekazać informacje:

1) kategorię odnośnych danych osobowych,
2) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych;

4. Spełnienie obowiązku informacyjnego, o którym mowa w ust. 3 nie ma zastosowania, gdy:

1) osoba, której dane dotyczą, dysponuje już tymi informacjami,
2) poinformowanie wymaga niewspółmiernie dużego wysiłku – w szczególności cele archiwizacyjne, statystyczne, badania naukowe,
3) przekazanie informacji okazuje się niemożliwe,
4) utrwalenie lub ujawnienie danych jest wyraźnie nakazane prawem UE lub prawem krajowym,
5) stanowią tajemnicę zawodową wynikającą z prawa UE lub prawa krajowego.
6) Powstanie obowiązku informacyjnego, o którym mowa w ust. 3 następuje w racjonalnym terminie po uzyskaniu danych osobowych, nie przekraczającym jednego miesiąca.
7) Obowiązki informacyjne, o których mowa w ust. 1 i 3 ADO nakłada na osoby zatrudnione przy przetwarzaniu danych osobowych.

§ 12.

Upoważnienia do przetwarzania danych osobowych

1. Administrator Danych Osobowych w Szkole przyznaje uprawnienia do przetwarzania danych osobowych gromadzonych w systemie tradycyjnym i informatycznym w formie imiennego upoważnienia.
2. Wzór upoważnienie, o którym mowa w ust. 1 stanowi **załącznik Nr 4** do niniejszej Polityki.
3. IOD zapewnia dla osób upoważnionych szkolenia z zakresu obowiązujących przepisów prawa i procedur wewnętrznych obowiązujących w Szkole.
4. Użytkownik systemu, użytkownik zewnętrzny po przeszkoleniu podpisuje oświadczenie o zachowaniu w tajemnicy danych, z którymi mają styczność oraz środkach bezpieczeństwa stosowanych przy przetwarzaniu danych osobowych oraz o zapoznaniu się z przepisami i procedurami. Wzór oświadczenia stanowi **załącznik nr 5** do Instrukcji.
5. Upoważnienie oraz oświadczenie przechowywane są w aktach osobowych pracownika oraz w dokumentacji IOD.
6. IOD prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych. Każda zmiana w zakresie informacji zawartych w ewidencji podlega niezwłocznemu odnotowaniu przez IOD. Wzór ewidencji stanowi **załącznik Nr 6** do Polityki.

§ 13.

Udostępnianie danych osobowych

1. ADO udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

2. Dane osobowe mogą być udostępniane w następujących przypadkach:

1) na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów;

2) na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych;

3) na podstawie wniosku osoby, której dane dotyczą.

3. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

4. W przypadku żądania udzielenia informacji na temat przetwarzanych danych osobowych na pisemny wniosek pochodzący od osoby, której dane dotyczą, odpowiedź na wniosek następuje w terminie miesiąca od daty jego otrzymania.

8. ADO odmawia udostępnienia danych osobowych, jeżeli spowodowałoby to:

1) ujawnienia wiadomości zawierających informacje niejawne,
2) zagrożenie dla obronności lub bezpieczeństwa państwa, życia lub zdrowia ludzi lub bezpieczeństwa publicznego,
3) zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa,
4) istotne naruszenia dóbr osobistych osób, których dane dotyczą, lub innych osób.

§ 14.

Powierzenie przetwarzania danych osobowych

1. Przetwarzanie dokonywane w imieniu ADO obywa się wyłącznie przez podmioty przetwarzające, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

2. Przetwarzanie przez podmiot przetwarzający odbywa się zgodnie z art. 28 RODO na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

3. Umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:

1) przetwarza dane osobowe wyłącznie na udokumentowane polecenie ADO; 2) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;

3) podejmuje wszelkie środki wymagane z zakresu bezpieczeństwa danych osobowych wynikających z przepisów RODO;

4) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego zgodnie z przepisami RODO;

5) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga ADO poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw;

6) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga ADO wywiązać się z obowiązków z zakresu bezpieczeństwa danych osobowych;

7) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji ADO usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo krajowe nakazują przechowywanie danych osobowych;

8) udostępnia ADO wszelkie informacje niezbędne do wykazania spełnienia określonych obowiązków oraz umożliwia ADO lub audytorowi upoważnionemu przez ADO przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

6. Umowa lub inny instrument prawny w celu zabezpieczenia Administratora zawiera w szczególności:

1) klauzule o zachowaniu poufności w umowie powierzenia,
2) zapisy dotyczące kar umownych,
3) zapisy o konieczności informowania ADO o kontrolach UODO u podmiotu przetwarzającego,
4) zapisy dotyczące możliwości przeprowadzenia kontroli przez Administratora u podmiotu,
5) zapisy dotyczące właściwego zakończenia współpracy,
6) informacja o incydentach w czasie 24 godzin po stwierdzeniu naruszenia.

7. IOD prowadzi ewidencję podmiotów przetwarzających, którym powierzono przetwarzanie danych.

8. Wzór ewidencji, o której mowa w ust. 7 stanowi **załącznik nr 7** do Polityki.

§ 15.

Środki organizacyjne ochrony danych osobowych stosowane w Szkole

1. Dostęp do danych wprowadzonych przez użytkowników systemów informatycznych mają jedynie upoważnione osoby oraz ADO zapewniający jego prawidłową eksploatację.

2. W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych wprowadza się następujące środki organizacyjne:

1) przetwarzanie danych osobowych w Szkole może odbywać się wyłącznie w ramach wykonywania zadań służbowych,

2) do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie,

3) dane osobowe powinny być wyłącznie przetwarzane w budynkach, pomieszczeniach do tego przystosowanych i zabezpieczonych, to znaczy posiadać odpowiednie zamki do drzwi oraz być wyposażone w środki ochrony ppoż., 4) każdy pracownik Szkoły uczestniczący w operacjach przetwarzania danych osobowych musi odbyć szkolenie z zakresu ochrony danych osobowych. Zasady prowadzenia szkoleń stanowią **załącznik nr 8** do niniejszej Polityki.

5) każdy upoważniony do przetwarzania danych osobowych w Szkole potwierdza fakt zapoznania się z niniejszą dokumentacją,

6) obszar przetwarzania danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych,

7) przebywanie osób, nieuprawnionych w ww. obszarze jest dopuszczalne za zgodą ADO lub w obecności osoby upoważnionej do przetwarzania danych,

8) pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz,

9) monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane,

10) zapewnienie bezpośredniego kontaktu pracownika z klientem oraz zapewnienie poufności i dyskrecji przy załatwianiu spraw – przy stanowisku pracownika znajduje się tylko osoba załatwiająca sprawę,

11) przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach.

§ 16.
Środki techniczne ochrony danych osobowych stosowane w Szkole

1. Dane osobowe przetwarzane w Szkole zabezpiecza się poprzez:

1) środki ochrony fizycznej:

a) przetwarzane dane osobowe przechowywane są w pomieszczeniach zabezpieczonych przed swobodnym dostępem.

b) budynek i pomieszczenia Szkoły posiadają następujące zabezpieczenia:

- wszystkie drzwi do pomieszczeń biurowych posiadają zamki na klucz,
- dokumenty z danymi osobowymi przechowywane są w szafach na akta wyposażonych w zamki na klucz.

2) środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:

a) czynności przetwarzania danych osobowych wykonywane są przy użyciu komputerów stacjonarnych, przenośnych,

b) zastosowano środki ochrony przed szkodliwym oprogramowaniem,

c) Szkoła posiada skonfigurowaną i zabezpieczoną przed spamem pocztę,

d) sieć komputerowa Szkoły podłączona jest do sieci Internet.

e) instalacja urządzeń systemu i sieci teleinformatycznej odbywa się za wiedzą i pod kontrolą ADO, który jest również odpowiedzialny za warunki wprowadzania do użycia, przechowywania, eksploatacji oraz wycofywania z użycia każdego urządzenia,

f) zabrania się na korzystanie z jakiegokolwiek nowego oprogramowania bez zgody Administratora.

3) środki ochrony w ramach systemowych narzędzi programowych i baz danych:

a) dostęp do baz danych wymaga uwierzytelnienia z wykorzystaniem spersonalizowanego identyfikatora użytkownika oraz unikatowego hasła użytkownika,

b) identyfikator użytkownika, który utracił dostęp do danych osobowych nie może być przydzielony innej osobie,

c) pierwsze hasło użytkownika jest ustalane przez ADO - nadającego uprawnienia dostępu w systemie informatycznym i przekazywane ustnie w odosobnionym miejscu bez osób trzecich,

d) hasło podlega szczególnej ochronie,

e) w przypadku podejrzenia, iż wiadomości o sposobie dostępu do elektronicznej bazy danych uzyskała osoba do tego niepowołana, osoba przetwarzająca dane w porozumieniu z ADO dokonuje zmiany hasła,

f) jednostka wykonuje okresowo kopie bezpieczeństwa danych osobowych ze wszystkich wykorzystanych w Szkole systemów informatycznych, programów, żeby zabezpieczyć przed utratą danych spowodowaną awarią sprzętu komputerowego,

g) komputery, serwery są zabezpieczone przed skutkami awarii bądź niestabilnego napięcia z sieci elektrycznej poprzez podłączenie wszystkich urządzeń do zasilacza UPS o mocy nie mniejszej jak 1500 VAT,

h) dyski twarde uszkodzone lub wyłączone z eksploatacji przed oddaniem do utylizacji należy trwale pozbawić zapisu lub zniszczyć dysk twardy w ten sposób, aby uniemożliwić odzyskanie informacji.

2. Wymagania dotyczące hasła:

1) autoryzacja w systemie operacyjnym odbywa się za pomocą hasła, które nie powinno zawierać mniej niż 8 znaków (używane małe i duże litery, cyfry oraz znaki specjalne),
2) autoryzacja w programach przetwarzających dane osobowe odbywa się za pomocą loginu i hasła, które nie powinno zawierać mniej niż 8 znaków (używane małe i duże litery, cyfry oraz znaki specjalne),
3) hasło nie może być takie samo jak identyfikator,
4) identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie,
5) hasło musi być zmieniane nie rzadziej niż 30 dni przez użytkownika, także w przypadku, gdy system informatyczny nie wymaga automatycznej zmiany,
6) użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności,
7) hasło przy wpisaniu nie może być wyświetlane na ekranie,
8) za gospodarkę identyfikatorami odpowiedzialny jest ADO,

9) zabronione jest stosowanie rozwiązań programowych pozwalających na zapamiętywanie identyfikatorów i haseł.

3. W przypadku zapomnienia hasła użytkownik powinien zwrócić się do ADO o wygenerowanie nowego hasła.
4. W przypadku podejrzenia zapoznania się z hasłem przez osobę nieuprawnioną użytkownik jest zobowiązany do natychmiastowej zmiany hasła oraz powiadomienia o zaistniałym fakcie ADO.

3. Przed rozpoczęciem pracy, w trakcie pracy oraz po jej zakończeniu należy zwrócić uwagę, czy nie występują przesłanki, mogące świadczyć o naruszeniu zasad ochrony danych osobowych, a w szczególności zachować procedury:

1) Procedura rozpoczęcia pracy:

a) rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje uruchomienie komputera, wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione,

b) użytkownik systemu jest odpowiedzialny za zabezpieczenie danych wyświetlanych przez system przed osobami niemającymi uprawnień.

2) Procedura zawieszenia pracy:

a) opuszczając stanowisko pracy (stację roboczą komputera) użytkownik zobowiązany jest dokonać zamknięcie używanych programów służących do przetwarzania danych osobowych oraz zapisać wszystkie otwarte dokumenty,

b) w przypadku czasowego opuszczenia stanowiska pracy, po 5 minutach uruchamia się automatycznie wygaszacz ekranu zabezpieczający hasłem. Monitory komputerów usytuowane są w miarę możliwości lokalowych w sposób uniemożliwiający odczytanie informacji z ekranu komputera osobom postronnym,

3) Procedura zakończenia pracy:

a) procedurę zakończenia pracy, należy rozpocząć od zamknięcia wszystkich używanych programów służących do przetwarzania danych osobowych oraz zapisać wszystkie otwarte dokumenty. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci,

b) użytkownik systemu nie powinien opuszczać stanowiska pracy do chwili wylogowania z systemu operacyjnego.

§ 17.

Konserwacje i naprawy

1. Przeglądy i konserwacje systemu informatycznego oraz nośników informacji służących do przetwarzania danych osobowych mogą być wykonywane jedynie przez osoby posiadające upoważnienia wydane przez Administratora Danych Osobowych (np. specjalistom z firm zewnętrznych).
2. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.
3. W przypadku uszkodzenia zestawu komputerowego, nośniki danych, na których są przechowywane dane osobowe powinny zostać zabezpieczone przez ADO.
4. W przypadku konieczności przeprowadzenia prac serwisowych poza Szkołą dane osobowe znajdujące się w naprawianym urządzeniu muszą zostać w sposób trwały usunięte - uniemożliwiający odczytanie danych lub nośnik na których się znajdują musi być usunięty z urządzenia na czas naprawy.
5. Jeżeli nie ma możliwości usunięcia danych z nośnika na czas naprawy komputera, należy zapewnić stały nadzór nad tym nośnikiem przez osobę upoważnioną do przetwarzania danych osobowych na nim zgromadzonych.
6. Zabronione jest dokonanie napraw sprzętu komputerowego samodzielnie przez pracowników. O wszelkich nieprawidłowościach lub awariach użytkownik systemu powinien niezwłocznie powiadomić ADO.

§ 18.

Plany awaryjne i zapobiegawcze

1. Serwer systemu oraz poszczególne stacje robocze (opcjonalnie) są zabezpieczone przed skutkami awarii bądź niestabilnego napięcia z sieci elektrycznej poprzez podłączenie wszystkich urządzeń do sieci elektrycznej zabezpieczonej centralnym UPS.

2. W celu zabezpieczenia ciągłości pracy, informacja przechowywana i przetwarzana w systemie podlegają archiwizacji przeprowadzanej z częstotliwością zapewniającą skuteczne ich zabezpieczenie.

3. Kopie archiwalne danych są wykonywane na nośnikach magnetooptycznych. Użycie kopii zapasowych następuje w przypadku odtwarzania systemu po awarii.

§ 19.

Postępowanie w przypadku naruszenia bezpieczeństwa ochrony danych osobowych

1. Naruszenie ochrony danych osobowych jest definiowane w art. 4 ust. 12 RODO jako naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
2. Procedura postępowania w sytuacji naruszenia ochrony danych osobowych stanowi **załącznik nr 6** do *Polityki Bezpieczeństwa Informacji Szkoły.*

§ 20.

Dokumentacja uzupełniająca Politykę Szkoły

Dokumentacja uzupełniająca politykę bezpieczeństwa w Szkole:

1) Wykaz pomieszczeń, w których przetwarzane są dane osobowe – załącznik nr 1 do Polityki,
2) Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe – załącznik nr 2 do Polityki,
3) Rejestr czynności przetwarzania danych osobowych – załącznik nr 3 do Polityki,
4) Upoważnienie i polecenie przetwarzania danych osobowych – załącznik nr 4 do Polityki,
5) Oświadczenie o poufności – załącznik nr 5 do Polityki,
6) Ewidencja osób upoważnionych do przetwarzania danych osobowych – załącznik nr 6 do Polityki,
7) Ewidencja podmiotów, którym powierzono przetwarzanie danych – załącznik nr 7 do Polityki,
8) Zasady prowadzenia szkoleń – załącznik nr 8.

§ 21.

Przepisy końcowe

1.Za naruszenie obowiązków wynikających z niniejszej Polityki oraz 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 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. , poz. 1781) może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym w szczególności wynikającym z przepisów tejże ustawy.

Art.107.1. Ustawy - *Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.*

Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.

Art. 82.1. RODO *Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.*

Art. 83. 1. RODO *Każdy organ nadzorczy zapewnia, by stosowane na mocny niniejszego artykułu za naruszenie niniejszego rozporządzenia administracyjne kary pieniężne, o których mowa w ust. 4, 5 i 6, były w każdym indywidulanym przypadku skuteczne, proporcjonalne i odstraszające.*

Art. 102. 1. UODO *Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 100 000 złotych, na:*

1) *jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1-12 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych;*
2) *Instytut badawczy;*
3) *Narodowy Bank Polski.*

2.W sprawach nie uregulowanych w niniejszej Polityce bezpieczeństwa przetwarzania danych osobowych mają zastosowanie przepisy 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 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).

POLITYKA POSTĘPOWANIA Z INCYDENTAMI ORAZ W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Definicja pojęć stosowanych w Polityce:

Stanowisko – pojedynczy komputer osobisty lub terminal przeznaczony do określonych zadań związanych między innymi z dostępem do sieci komputerowej Szkoły.

System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Zasoby informatyczne – ogół systemów informatycznych wykorzystywanych przez daną organizację.

Incydent związany z bezpieczeństwem informacji – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań statutowych Szkoły i zagrażają bezpieczeństwu informacji.

Podatność – słabość systemu informatycznego, która może być wykorzystana przez co najmniej jedno zagrożenie.

2. Cel polityki

Celem Polityki jest zapewnienie, by zdarzenia związane z bezpieczeństwem informacji oraz słabości systemów informatycznych zostały zgłaszane w sposób umożliwiający szybkie podjęcie działań korygujących.

3. Zakres stosowania

Działania opisane w niniejszej Procedurze obowiązują wszystkich użytkowników systemów tradycyjnych i informatycznych.

4. Istota naruszenia danych osobowych

1. Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
2. Incydentem z zakresu bezpieczeństwa informacyjnego nazywa się pojedyncze, niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria

takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań i zagrażają bezpieczeństwu informacji.

3. Każde naruszenie ochrony danych osobowych jest incydentem, ale nie każdy incydent stanowi naruszenie w rozumieniu przepisów o ochronie danych osobowych.

5. Klasyfikacja incydentów

Polityka postępowania z incydentami powinna obejmować incydenty typu:

1. awaria systemów informacyjnych,
2. utrata usługi,
3. wykrycie kodu złośliwego,
4. odmowa usługi,
5. naruszenie poufności i integralności,
6. niewłaściwe użycie systemów informacyjnych,
7. oszustwa komputerowe,
8. obraźliwe i nielegalne treści,
9. próby włamań.

Naruszenie bezpieczeństwa informacji może być spowodowane:

1. niewłaściwym oddziaływaniem czynników zewnętrznych, takich jak: temperatura otoczenia, wilgotność, pole elektromagnetyczne, wirusy komputerowe, skutki powodzi, pożaru, itp.,
2. niekontrolowanym działaniem osób trzecich, powodującym zakłócenia systemu podczas włamania, niewłaściwym działaniem zespołów serwisowych, przetwarzaniem danych bez uprawnień, tworzeniem w zbiorach użytkownika nieautoryzowanych kont dostępu,
3. umyślnym lub nieumyślnym działaniem a nawet zaniechaniem działania użytkowników przetwarzających dane lub osób odpowiedzialnych za ich ochronę.

Za naruszenie bezpieczeństwa informacji uważa się w szczególności:

1. brak możliwości fizycznego dostępu do danych np. zagubiony klucz do pomieszczenia lub mebli biurowych, w których przechowywane są dokumenty, zniszczona szafa z dokumentami, brak nośników informacji, zalane pomieszczenie, brak sprzętu komputerowego itp.,
2. brak dostępu do danych,
3. niepoprawną treść, postać datę, różnicę w danych itp.,

4. próbę lub fakt nieuprawnionego dostępu do danych lub pomieszczenia, w których dane są przetwarzane np. zmiana kolejności dokumentów, otwarte drzwi lub meble biurowe, nietypowe ustawienie sprzętu lub pojawienie się nowych dokumentów,
5. różnice funkcjonowania systemu a w szczególności wyświetlania komunikatów i informacji o błędach oraz nieprawidłowościach w wykonaniu operacji,
6. zniszczenie lub próby zniszczenia, w sposób nieautoryzowany danych ze zbioru danych lub danych systemowych,
7. nieskuteczne niszczenie nośników informacji umożliwiające ponowny ich odczyt przez osoby nieuprawnione,
8. zmianę lub utratę danych zapisanych na kopiach awaryjnych lub zapisach archiwalnych,
9. próba nielegalnego logowania się do systemu lub włamania do systemu,
10. zmienione oprogramowanie systemu, stwierdzone przez użytkownika po przerwie w przetwarzaniu danych.

6. Przykłady zagrożeń i incydentów

Przykładowy katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych z określeniem obowiązku notyfikacji:

Rejestr wewnętrzny	Notyfikacja – obwiązek zgłoszenia do UODO
utrata zaszyfrowanego komputera; przesłanie zaszyfrowanego załącznika do nieuprawnionych osób; otrzymanie informacji, dla których nie mamy podstawy prawnej do ich przetwarzania; przekazanie dokumentacji osobie, która nie jest upoważniona do ich przetwarzania; niedostępność systemów IT, która nie ma wpływa na osoby; niewylogowanie się przed opuszczeniem stanowiska pracy; samodzielne instalowanie i wykorzystanie nielegalnego oprogramowania oraz narzędzi służących do obchodzenia zabezpieczeń w systemach informatycznych; wykorzystanie służbowej poczty	kradzież danych z systemu IT; nieuprawniony dostęp do danych osobowych po upgrade systemu IT; utrata niezaszyfrowanego nośnika z danymi osobowymi zawierającymi dane szczególne; usunięcie danych, które powinny być dalej przetwarzane; niedostępność systemów IT wpływająca na osoby; nieprawidłowa anonimizacja danych; zmiana konfiguracji sprzętowej oraz programowej systemów oraz stacji roboczych przez niepowołane osoby; utrata kontroli nad kopią danych osobowych; kradzież komputerów lub twardych dysków z danymi osobowymi; udostępnienie danych osobowych osobom nieupoważnionym w formie

elektronicznej do celów prywatnych; pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru; przechowywanie dokumentów zabezpieczonych w niedostatecznym stopniu przed dostępem osób niepowołanych; dopuszczenie, aby osoby postronne odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe; opuszczenie i pozostawienie bez dozoru niezamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych; wpuszczenie do pomieszczenia osób nieznanych i dopuszczenie ich do kontaktu ze sprzętem komputerowym; pozostawienie otwartych okien i drzwi po zakończeniu pracy; nieprzestrzeganie zasady czystego biurka; pozostawienie dokumentów w koszu na śmieci- dokumentacja jest niszczona bez użycia niszczarki; pozostawienie wydruków na drukarce; ślady manipulacji przy układach sieci komputerowej lub komputerach; ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe; przechowywanie haseł w niewłaściwy sposób; przekazywanie haseł innym osobom; niewłaściwe niszczenie nośników z	papierowej, elektronicznej lub ustnej.

danymi pozwalającymi na ich odczyt; fizyczne zniszczenie lub uszkodzenie sprzętu oraz nośników przetwarzających dane; pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów; maile zachęcające do ujawnienia identyfikatora i/lub hasła; telefoniczne próby wyłudzenia danych osobowych.	

7. Postępowanie z incydentami oraz w przypadku naruszenia danych osobowych

1. Każdy użytkownik, który stwierdzi lub podejrzewa fakt zauważenia incydentu lub naruszenia danych osobowych jest zobowiązany niezwłocznie, **nie później niż w ciągu tego samego dnia od stwierdzenia lub podejrzenia faktu** zgłosić to ADO oraz Inspektorowi Ochrony Danych, wypełniając wewnętrzny formularz zgłoszenia, stanowiący **załącznik nr 1** do niniejszej Procedury.
2. Każdy użytkownik, który stwierdzi fakt incydentu lub naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia.
3. W przypadku stwierdzenia incydentu lub naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia IOD, ADO lub innej osoby upoważnionej przez niego.
4. Inspektor ochrony danych podejmuje następujące kroki:
   1) zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy;
   2) odbiera pisemne wyjaśnienia z zaistniałego naruszenia bezpieczeństwa danych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym incydentem lub naruszeniem;

3) dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając raport z naruszenia **- załącznik nr 2** do Procedury;
4) dokonuje rejestracji incydentu w wewnętrznym rejestrze, stanowiącym **załącznik nr 3** o niniejszej Procedury.

5. W przypadku naruszenia danych osobowych IOD przedstawia zebrane materiały Administratorowi, który z pomocą IOD w terminie i na podstawie przesłanek określonych w ogólnym rozporządzeniu o ochronie danych ocenia, czy zaistniałe naruszenie podlega obowiązkowi zgłoszenia organowi nadzorczemu oraz powiadomieniu osoby, której dane dotyczą.
6. Czynnikiem warunkującym obowiązek zgłoszenia naruszenia Prezesowi Urzędu Ochrony Danych Osobowych jest ryzyko naruszenia praw i wolności osób fizycznych, które istnieje, gdy naruszenie może skutkować fizyczną, materialną lub niematerialną szkodą dla osób fizycznych, których dane naruszono. Przykładem takich szkód jest dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne.
7. Dokonując analizy pod kątem ryzyka naruszenia praw lub wolności osób fizycznych należy uwzględnić następujące czynniki:
   1) rodzaj naruszenia,
   2) charakter, wrażliwość i ilość danych osobowych,
   3) łatwość identyfikacji osób fizycznych,
   4) powaga konsekwencji dla osób fizycznych,
   5) cechy szczególnie osoby fizycznej (np. dzieci, osoby wymagające szczególnej opieki – osoby starsze),
   6) cechy szczególne administratora danych,
   7) liczba osób fizycznych, których dane naruszono.
8. W przypadku stwierdzenia, że naruszenie należy zgłosić Prezesowi Urzędu Ochrony Danych Osobowych, Administrator dokonuje tego bez zbędnej zwłoki, nie później jednak niż w

terminie 72 godzin po stwierdzeniu naruszenia. Do zgłoszenia przekazanego organowi nadzorczemu po ustawowym terminie dołącza się wyjaśnienie przyczyn opóźnienia.

9. Zgłoszenie, o którym mowa w ust. 8 przygotowuje Inspektor Ochrony Danych za pomocą odpowiedniego elektronicznego formularza dostępnego na stronie https://uodo.gov.pl.
10. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą o takim naruszeniu.
11. Zawiadomienie, o którym mowa w ust. 10 przygotowuje IOD, który jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych, możliwe konsekwencje naruszenia ochrony danych osobowych, środki zastosowane lub proponowane w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosowanych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków oraz wskazuje własne dane tj. imię i nazwisko oraz dane kontaktowe.
12. Zawiadomienie, o którym mowa w ust. 10 i 11, nie jest wymagane, w następujących przypadkach:
    1) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,
    2) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
    3) Wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.
13. Inspektor ochrony danych prowadzi pełną dokumentację Administratora dotyczącą wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania przepisów.

8. Odpowiedzialność

1. Odpowiedzialność za prawidłowe zgłoszenie incydentów dotyczących bezpieczeństwa infrastruktury informatycznej oraz naruszeń ochrony danych osobowych spoczywa użytkownikach systemów tradycyjnych i informatycznych upoważnionych do przetwarzania danych osobowych.

2. ADO odpowiedzialny za rozwiązanie problemu lub zapobieżenie incydentowi działa zgodnie z niniejszą procedurą.

3. Wobec osoby, która w przypadku naruszenia danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, wszczyna się postępowanie dyscyplinarne lub porządkowe.

4. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.

5. Kara dyscyplinarna wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z aktualnie obowiązującymi przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

POLITYKA PROFILAKTYKI ANTYWIRUSOWEJ

1. Ochrona systemu informatycznego przed wirusami komputerowymi

Wszystkie komputery są narażone na działanie złośliwego oprogramowania (wirusy komputerowe). Wirusy komputerowe mogą dostać się do komputera poprzez: elektroniczne nośniki informacji, e-mail, strony internetowe, sieć komputerową. W komputerze musi być zainstalowany działający w „tle" program antywirusowy, który automatycznie sygnalizuje obecność wirusów, w trakcie włączania systemu lub wprowadzania danych z zewnętrznych nośników informacji. W komputerze musi być zainstalowany firewall, chroniący komputer przed atakami z zewnątrz. Kontrola antywirusowa systemu obejmować powinna:

1. Wszystkie elektroniczne nośniki informacji,
2. E-maile,
3. Strony internetowe,
4. Ściągane pliki z Internetu.

Na komputerach, na których są przetwarzane dane osobowe, mogą być otwierane tylko dozwolone strony internetowe. Komputery te łączą się z Internetem poprzez urządzenie UTM. Kategorie stron dozwolonych i blokowanych są skonfigurowane na urządzeniu UTM.

Osobą prowadzącą działania profilaktyczne mające na celu ochronę zasobów sieci komputerowej Zespołu Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz przed atakami wirusów komputerowych jest ADO.

Zasoby informatyczne są skanowane na bieżąco za pomocą modułu rezydentnego. Kontroli podlegają wszystkie pliki (odczytywane i zapisywane), w tym poczta elektroniczna. System antywirusowy jest zaprogramowany do wykonywania okresowych kontroli antywirusowych całego systemu plików. Kontrole te są wykonywane przez program automatycznie nie rzadziej niż jeden raz w tygodniu.

Zabrania się korzystania ze stanowiska bez aktywnego programu antywirusowego.

2. Postępowanie w przypadku ujawnienia lub podejrzenia istnienia wirusa

Gdy zachowanie systemu komputerowego odbiega od normy (komunikaty o błędach, nieoczekiwane zamknięcie lub pojawienie się plików lub katalogów, spowolniona praca systemu, dziwne lub niezrozumiałe informacje pojawiające się na ekranie itp.) należy również przeprowadzić kontrolę antywirusową systemu.

Jeżeli program antywirusowy stwierdził istnienie wirusa na nośniku danych, taki nośnik należy natychmiast wyjąć z czytnika (stacji czytnika DVD-ROM, USB itp.) wyraźnie oznaczyć i przekazać nośnik ADO oraz przeprowadzić kontrolę antywirusową całego systemu.

Po stwierdzeniu obecności wirusa w systemie przez program antywirusowy, jeśli to możliwe, należy zezwolić programowi antywirusowemu na usunięcie wirusów. Jeśli program antywirusowy nie będzie mógł usunąć wirusów nie niszcząc części lub całości zbioru zainfekowanego wirusem, należy przerwać działanie programu antywirusowego i natychmiast zgłosić ten fakt ADO.

Użytkownik ma obowiązek zgłaszania do ADO wszelkich zauważonych niestandardowych zachowań systemu antywirusowego.

POLITYKA TWORZENIA KOPII ZAPASOWYCH

1. Definicja pojęć stosowanych w Polityce:

Stanowisko – pojedynczy komputer osobisty lub terminal przeznaczony do określonych zadań związanych między innymi z dostępem do sieci komputerowej Zespołu Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz.

Zasoby informatyczne – ogół systemów informatycznych wykorzystywanych przez daną organizację.

Kopia zapasowa – kopia danych lub oprogramowania. Celem jej wykonywania jest odtworzenie systemu po awarii.

2. Cel polityki

Polityka Tworzenia Kopii Zapasowych określa zasady tworzenia, przechowywania i testowania kopii zapasowych oraz odzyskiwania z nich danych i systemów informatycznych, w celu zapewnienia integralności i dostępności informacji oraz środków przetwarzania informacji.

3. Wykonywanie kopii systemów informatycznych

Na potrzeby zachowania ciągłości działania systemów informatycznych i utrzymania integralności danych, wykonuje się kopie zapasowe zbiorów danych, w tym danych osobowych.

Ochronie poprzez wykonywanie kopii podlegają także programy i narzędzia programowe służące przetwarzaniu danych. Kopie programów i narządy wykonywane są zaraz po instalacji oraz po każdej aktualizacji na zewnętrznych elektronicznych nośnikach informacji.

Kopie zapasowe baz danych stosowanych w Zespole Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz systemów, programów, aplikacji sporządza systematycznie ADO.

W przypadku lokalnego przetwarzania danych, w tym danych osobowych na stacjach roboczych, użytkownicy systemu informatycznego zobowiązani są do wykonania samodzielnego kopii bezpieczeństwa zbiorów.

Kopie zapasowe mogą być wykonywane tylko na nośnikach informatycznych zaakceptowanych przez ADO.

Kopie zapasowe konfiguracji systemów operacyjnych serwerów wykonuje ADO po każdej zmianie konfiguracji oprogramowania (np. po utworzeniu, rekonfiguracji lub usunięciu konta użytkownika w systemie, zmianie praw dostępu itp.).

Kopie zapasowe sprawdzane są okresowo pod kątem ich dalszej przydatności nie rzadziej niż raz w roku. Polega to na testowym odtworzeniu zawartości kopii na innym urządzeniu. Po stwierdzeniu nieprzydatności kopii zapasowych zbiorów nośnik zostaje pozbawiony danych lub wybrakowany w inny sposób uniemożliwiający dalszy odczyt informacji.

Niedopuszczalne jest przechowywanie kopii zapasowych na tych samych nośniach, na których są one przetwarzane.

Za prawidłowe tworzenie kopii zapasowych odpowiada ADO.

4. Odzyskiwanie danych i systemów informatycznych z kopii zapasowych

Odzyskiwanie danych z kopii zapasowych jest wykonywane w następujących przypadkach:

a) utraty całości lub części danych na serwerze,
b) utraty integralności całości lub części danych na serwerze,
c) w celu odtworzenia poprzedniej wersji danych na wniosek użytkownika,
d) na wniosek organu kontrolnego (np. NIK),
e) przy przenoszeniu danych na nowy serwer,
f) przy przenoszeniu na nową jednostkę komputerową.

Odzyskiwanie całego systemu informatycznego jest wykonywane w wypadku awarii sprzętowej lub systemowej nośników danych, na których jest on zlokalizowany, uniemożliwiającej korzystanie z danego systemu.

Za odzyskiwanie danych z kopii zapasowych odpowiada ADO.

POLITYKA ZARZĄDZANIA RYZYKIEM I OCENA SKUTKÓW DLA PRZETWARZANIA DANYCH

1. Wstęp

Mając na uwadze konieczność uwzględnienia w procesie przetwarzania danych osobowych prawdopodobieństwa i powagi ryzyka naruszenia praw lub wolności osób, których przetwarzanie dotyczy, ADO niniejszym dokumentem wprowadza do organizacji procedurę szacowania ryzyka w stosunku do aktualnie prowadzonych jak i planowanych operacji przetwarzania danych osobowych.

ADO ma świadomość odpowiedzialności prawnej w kontekście przetwarzanych danych osobowych, dlatego wdraża takie środki techniczne i organizacyjne, które zapewnią bezpieczeństwo przetwarzanych danych osobowych. Zastosowane środki techniczne i organizacyjne są poddawane cyklicznemu doskonaleniu.

2. Cel szacowania ryzyka

1. ADO przeprowadza proces szacowania ryzyka w zakresie bezpieczeństwa informacji w celu zidentyfikowania obszarów, które mogą istotnie wpływać na osobę, której przetwarzanie dotyczy. ADO wdraża podejście oparte na ryzyku, aby zapewnić ochronę praw i wolności osób, których przetwarzanie dotyczy.
2. Na szacowanie ryzyka składa się:
   1) Analiza Ryzyka Ogólnego,
   2) Ocena Skutków Dla Przetwarzania Danych (DPIA).
3. **Definicje:**

Określenia i skróty użyte w Polityce:

1. **Szacowanie ryzyka** – rozumie się przez to proces analizy i oceny ryzyka. W procesie szacowania ryzyka w kontekście danych osobowych szacowanie ryzyka uwzględnia ryzyka związane z naruszeniem praw i wolności osób fizycznych, których przetwarzanie dotyczy;
2. **Analiza ryzyka** – rozumie się przez to proces identyfikacji źródeł ryzyka i oszacowania ryzyka;
3. **Ocena ryzyka** – proces porównywania oszacowanego ryzyka w celu określenia znaczenia ryzyka;
4. **Ryzyko** – rozumie się przez to kombinację prawdopodobieństwa zdarzenia i jego konsekwencji;

5. **Ryzyko szczątkowe** – rozumie się przez to ryzyko pozostające po procesie postępowania z ryzykiem;
6. **Postępowanie z ryzykiem** – rozumie się przez to proces zmiany poziomu ryzyka poprzez zastosowanie odpowiednich środków technicznych i organizacyjnych;
7. **Akceptacja ryzyka** – rozumie się przez to decyzję ADO o tym, aby ryzyko zaakceptować;
8. **Podatność** – rozumie się przez to słabość w strukturze fizycznej, technicznej, organizacyjnej organizacji;
9. **Incydent** – rozumie się przez to zdarzenie mające lub mogące mieć negatywny wpływ na System Zarządzania Bezpieczeństwem Informacji w organizacji. Incydent może powodować w stosunku do osoby fizycznej, której dane osobowe organizacja przetwarza, szkodę o charakterze majątkowym lub niemajątkowym;
10. **Poufność** – rozumie się przez to właściwość polegająca na tym, że osoba nieupoważniona bądź podmiot nie mają dostępu do danych osobowych, które temu atrybutowi podlegają;
11. **Integralność** – rozumie się przez to właściwość polegająca na tym, że aktywa w postaci informacji/danych osobowych pozostają kompletne;
12. **Dostępność** – rozumie się przez to właściwość polegająca na tym, że aktywa w postaci informacji/danych osobowych pozostają dostępne dla osób upoważnionych /uprawnionych do ich przetwarzania;
13. **Bezpieczeństwo informacji** – rozumie się przez to zachowanie wobec przetwarzanych danych osobowych/informacji takich atrybutów jak poufność, integralność oraz dostępność.

4. Oznaczenie uwarunkowań związanych z funkcjonowaniem organizacji – ustalenie kontekstu

1. Organizacja określa, które z uwarunkowań zewnętrznych bądź wewnętrznych mają znaczenie dla szacowania ryzyka.
2. Uwarunkowania zewnętrzne istotnie wpływające na organizację:
    1) relacje z innymi administratorami danych osobowych,
    2) relacje z innymi podmiotami zewnętrznymi,
    3) zasięg terytorialny działalności organizacji,
    4) uwarunkowania prawne organizacji.
3. Uwarunkowania wewnętrzne istotnie wpływające na organizację:
    1) struktura i rozmiary organizacji,

2) uwarunkowania formalne wewnętrzne (polityki, regulaminy),
3) sposoby podejmowania decyzji w organizacji względem bezpieczeństwa przepływu danych,
4) kultura organizacji.

4. Organizacja na etapie tworzenia Polityki Bezpieczeństwa Informacji przeanalizowała:

1) podstawy legalności przetwarzania danych (w oparciu o przesłanki wynikające z RODO),
2) staranność po stronie organizacji w zakresie spełniania obowiązków informacyjnych oraz realizacji praw osób fizycznych, których dane osobowe dotyczą w oparciu o RODO,
3) cel przetwarzania danych osobowych,
4) zakres przetwarzanych danych kierując się zasadami przetwarzania danych określonymi w RODO,
5) wymagania dotyczące zabezpieczeń organizacyjnych, środków kontroli logicznej procesu przetwarzania, środków ochrony fizycznej danych.

5. Wybór metody na cele przeprowadzenia Analizy Ryzyka Ogólnego i Oceny Skutków dla Przetwarzania Danych.

1. Rozporządzenie ogólne o ochronie danych pozostawia ADO wybór w zakresie zastosowania konkretnej metody szacowania ryzyka.

2. ADO ma świadomość, iż w procesie szacowania ryzyka może kierować się metodą:

1) ilościową: wielkość poniesionych strat próbuje się wyrazić liczbowo, niejednokrotnie w oparciu o dane statystyczne bądź,

2) jakościową: wielkość zagrożenia ocenia się przez pryzmat doświadczenia oraz intuicji osoby szacującej ryzyko (subiektywne odczucie).

3. ADO ma świadomość, iż szacowanie ryzyka w procesie przetwarzanych danych osobowych powinno opierać się o metodę jakościową - strat związanych z ochroną danych osobowych bardzo często nie sposób wyrazić za pomocą liczb.

4. Atrybuty, jakie ADO przyjmuje w tabeli szacowania ryzyka to:

1) Poufność – osoba nieupoważniona bądź nieupoważniony podmiot nie mają dostępu do danych osobowych. Dane osobowe zgodnie z tym atrybutem nie są ujawniane w nieuprawniony sposób.

2) Integralność – konieczność zapewnienia spójności danych osobowych; atrybut determinujący konieczność ochrony danych osobowych przed przypadkowym ich zniekształceniem w przypadku ich zapisu, odczytu, transmisji bądź magazynowania.

3) Dostępność – zasób w postaci danych osobowych jest możliwy do wykorzystania na żądanie w konkretnym czasie przez osobę bądź podmiot upoważniony/uprawniony w zakresie dostępu do danych.

6. Klasyfikacja czynności przetwarzania

1. ADO, w pierwszej kolejności dzieli czynności przetwarzania na te, które wymagają Oceny Skutków dla Przetwarzania Danych (DPIA) oraz te, względem których ADO wykonuje Analizę Ryzyka Ogólnego.

2. Kryterium, według którego ADO dokonuje wstępnej klasyfikacji z uwzględnieniem kontekstu przetwarzania danych są wytyczne Grupy Roboczej art. 29 WP 248 rew.01 17/PL dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie może powodować wysokie ryzyko do celów rozporządzenia 2016/679 tj.:

1) Ocena lub punktacja: w tym profilowanie i prognozowanie w szczególności na podstawie „aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą" (motywy 71 i 91).

2) Automatyczne podejmowanie decyzji o skutku prawnym lub podobnie znaczącym skutku: przetwarzanie mające na celu podjęcie decyzji w sprawie osób, których dane dotyczą, wywołujących „skutki prawne wobec osoby fizycznej" lub decyzji, które „w podobny sposób istotnie na nią wpływają" (art. 35 ust. 3 lit. a)). Zagrożenie: przetwarzanie mogące prowadzić do wykluczenia lub dyskryminacji osób fizycznych. Przetwarzanie mające niewielki wpływ na osoby fizyczne lub niemające na nie żadnego wpływu nie spełnia tego konkretnego kryterium.

3) Systematyczne monitorowanie: przetwarzanie wykorzystywane do obserwacji, monitorowania lub kontrolowania osób, których dane dotyczą, w tym danych gromadzonych za pośrednictwem sieci lub ramach „systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie" (art. 35 ust. 3 lit. c)). Zagrożenie: osoby, których dane dotyczą, nie są świadome tego, kto gromadzi ich dane i w jaki sposób z nich korzysta. Ponadto osoby fizyczne mogą nie być w stanie uniknąć takiego rodzaju przetwarzania w przestrzeni publicznej (lub przestrzeni publicznie dostępnej).

4) Dane wrażliwe lub dane o charakterze wysoce osobistym: obejmują szczególne kategorie danych osobowych określone w art. 9 oraz dane osobowe dotyczące

wyroków skazujących za przestępstwo lub naruszeń prawa zdefiniowane w art. 10.

5) Dane przetwarzane na dużą skalę: przy ustalaniu, czy przetwarzanie danych odbywa się na dużą skalę, ADO we współpracy z Inspektorem Ochrony Danych bierze pod uwagę w szczególności następujące czynniki:

a) liczbę osób, których dane dotyczą – wyrażoną jako konkretna wartość albo jako odsetek populacji odniesienia;

b) ilość danych lub zakres poszczególnych przetwarzanych pozycji danych;

c) czas trwania lub trwałość czynności przetwarzania danych;

d) zakres geograficzny czynności przetwarzania.

6) Dopasowywanie lub łączenie zbiorów danych: zbiory pochodząc z co najmniej dwóch operacji przetwarzania danych przeprowadzonych w różnych celach lub przez różnych administratorów danych w sposób wykraczający poza uzasadnione oczekiwania osób, których dane dotyczą.

7) Dane dotyczące osób wymagających szczególnej opieki, których dane dotyczą: przetwarzanie tego rodzaju danych stanowi jedno z kryteriów ze względu na zwiększoną nierównowagę sił między osobami, których dane dotyczą, a administratorem danych, co oznacza, że osoby fizyczne mogą mieć trudności z wyrażeniem zgody na przetwarzanie swoich danych lub z wyrażeniem sprzeciwu wobec ich przetwarzania, lub mogą mieć trudności z korzystaniem z przysługujących im praw. Do osób wymagających szczególnej opieki, których dane dotyczą, zalicza się dzieci, pracowników, bardziej wrażliwe grupy społeczne wymagające szczególnej ochrony oraz w każdą sytuację, gdy można stwierdzić brak równowagi między stanowiskiem osoby, której dane dotyczą, a stanowiskiem administratora.

8) Innowacyjne wykorzystanie lub stosowanie nowych rozwiązań technologicznych lub organizacyjnych, takich jak połączenie technologii rozpoznającej odcisk palca i twarz w celu poprawy fizycznej kontroli dostępu. Zastosowanie takiej technologii może wiązać się z nowymi formami gromadzenia i wykorzystania danych, co może stwarzać ryzyko naruszenia praw i wolności osób fizycznych. Ocena skutków dla ochrony tych danych pomoże Administratorowi zrozumieć ryzyko i je wyeliminować.

9) Gdy samo przetwarzanie „uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy”. Obejmuje to operacje przetwarzania, których celem jest umożliwienie osobom, których dane dotyczą,

uzyskania dostępu do usługi lub zawarcia umowy, zmiana tego dostępu lub odmówienie dostępu.

3. Ocena Skutków dla Przetwarzania Danych (DPIA) nie jest obowiązkowa w przypadkach:

1) gdy nie jest prawdopodobne, aby operacja przetwarzania może powodować wysokie ryzyko,

2) gdy przeprowadzono już podobną ocenę skutków dla ochrony danych,

3) gdy operację przetwarzania zatwierdzono przed majem 2018 r.,

4) gdy operacja przetwarzania posiada podstawę prawną, która reguluje daną operację przetwarzania,

5) gdy operacja przetwarzania znajduje się w wykazie operacji przetwarzania, które nie podlegają ocenie skutków dla ochrony danych.

4. **„Klasyfikacja Czynności Przetwarzania do Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA)”** – dokument stanowiący **Załącznik nr 1** do **Polityki Zarządzania Ryzykiem i Ocena Skutków dla Przetwarzania Danych**, określa czynności przetwarzania względem których należy przeprowadzić analizę ryzyka ogólnego oraz czynności przetwarzania, względem których należy przeprowadzić ocenę skutków.

6. Grupowanie podobnych czynności przetwarzania

1. Zgodnie z art. 35 ust. 1 RODO dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem Administrator przeprowadza pojedynczą ocenę.

2. Administrator grupuje podobne operacje przetwarzania dla Analizy ryzyka ogólnego (ARO) oraz Oceny Skutków Przetwarzania Danych (DPIA) uwzględniając kontekst ich przetwarzania w oparciu o następujące kryterium:

1) ARO-Gr.1 - dane osobowe związane z pracownikami,

2) ARO-Gr.2 - dane osobowe związane z usługami "na zewnątrz" (np. czynności dla społeczeństwa, oferta kulturalna, zajęcia, konkursy itd.),

3) ARO-Gr.3 - dane osobowe związane z usługami "do wewnątrz" (np. kontrahenci, usługodawcy itp.),

4) DPIA-Gr.1 - dane osobowe związane z pracownikami,

3. Przedmiotowe grupowanie podobnych operacji przetwarzania znajduje odzwierciedlenie w „Grupowaniu podobnych czynności przetwarzania do Analizy Ryzyka Ogólnego i Oceny Skutków dla Przetwarzania Danych (DPIA)” – dokumencie

stanowiącym Załącznik nr 2 do Analizy Ryzyka Ogólnego i Oceny Skutków dla Przetwarzania Danych (DPIA).

7. Szacowanie ryzyka

1. Proces szacowania ryzyka Administrator poprzedza identyfikacją aktywów organizacji, zagrożeń dla aktywów, zabezpieczeń stosowanych w organizacji, podatności (prawdopodobieństwa) oraz następstw (skutków).

2. **Organizacja identyfikuje aktywa** i dzieli je na aktywa podstawowe i aktywa wspierające.

   1) Do aktywów podstawowych organizacja zalicza:

      a) informacje - obejmują dane osobowe, które organizacja przetwarza w związku z prowadzoną działalnością; informacje niezbędne do ociągnięcia celów organizacji,

      b) operacje przetwarzania: czynności w procesie przetwarzania danych osobowych, które organizacja jest zobowiązana podejmować/utrzymywać, by osiągać cele strategiczne jednostki przy jednoczesnym zapewnieniu bezpieczeństwa przetwarzanych informacji w organizacji.

   2) Do aktywów wspierających organizacja zalicza:

      a) sprzęt - obejmuje przenośne oraz stacjonarne urządzenia komputerowe, urządzenia serwerowe, urządzenia peryferyjne (drukarki czy wymienny napęd dyskowy),

      b) nośniki danych (papierowe) zawierające dane osobowe - dokumentacja zawierająca treści o charakterze osobowym,

      c) nośniki danych (elektroniczne) - z racji swojego przeznaczenia mogą być podłączone do urządzenia komputerowego w celu przygotowania danych osobowych do przetwarzania (pendrive, płyta CD ROM, wymienny dysk twardy),

      d) oprogramowanie - obejmuje wszystkie programy, dzięki którym bądź w oparciu o nie organizacja przetwarza dane osobowe. W zakresie oprogramowania uwzględnia się system operacyjny, oprogramowanie uzupełniające usługi systemu operacyjnego, oprogramowanie służące do obsługi poczty elektronicznej czy bazy danych, standardowe i dedykowane aplikacje biznesowe np. oprogramowanie księgowe, oprogramowanie służące do obsługi Klientów, pracowników organizacji.

e) okablowanie - sieć, którą należy rozumieć przez pryzmat urządzenia używanego do połączenia wielu komputerów i elementów systemu informacyjnego,

f) personel – osoby zaangażowane w proces przetwarzania danych osobowych oraz obsługę systemu informacyjnego. Do personelu zaliczamy kierownictwo, osoby upoważnione do przetwarzania danych, osoby, którym nadano uprawnienia do pracy w programach dziedzinowych bazodanowych, osoby, które mają w zakresie swoich obowiązków mają między innymi konieczność utrzymania systemu informacyjnego oraz twórców oprogramowania,

g) lokalizację - siedziba, ale również środowisko zewnętrzne. Siedziba organizacji odnosi się do budynków, jakie organizacja zajmuje oraz wszystkich obszarów przetwarzania wewnątrz budynków. Siedziba jest istotna ze względu na jej położenie geograficzne, obszar miejski, przestrzeń publiczną.

3. Organizacja identyfikuje zagrożenia i dzieli je na:

1)zniszczenia fizyczne:

a) pożar,
b) zalanie,
c) zanieczyszczenie,
d) poważny wypadek,
e) zniszczenie urządzeń lub nośników,
f) pył, korozja, wychłodzenie.

2)zjawiska naturalne:

a) zjawiska klimatyczne,
b) zjawiska sejsmiczne,
c) zjawiska pogodowe,
d) powódź.

3)utrata podstawowych usług:

a) utrata dostaw prądu,
b) awaria urządzenia telekomunikacyjnego.

4)naruszenia bezpieczeństwa informacji:

c) podsłuch,
d) kradzież nośników lub dokumentów,
e) kradzież urządzenia,
f) sfałszowanie oprogramowania,

5)awarie techniczne:

a) awaria urządzenia,
b) niewłaściwe funkcjonowanie urządzeń,
c) przeciążenie systemu informacyjnego,
d) niewłaściwe funkcjonowanie oprogramowania,
e) naruszenie zdolności utrzymania systemu informacyjnego.

6)nieautoryzowane działania:

a) nieautoryzowane użycie urządzeń,
b) nieuprawnione kopiowanie oprogramowania,
c) użycie fałszywego lub skopiowanego oprogramowania,
d) zniekształcenie danych,
e) nielegalne przetwarzanie danych.

7)naruszenia bezpieczeństwa funkcji:

a) błąd użytkowania,
b) naruszenie praw,
c) fałszowanie praw,
d) naruszenie dostępności personelu.

5. Organizacja identyfikuje podatność (prawdopodobieństwo) wystąpienia zdarzenia w organizacji zgodnie z poniższą skalą:

PRAWDOPODOBIEŃSTWO	SKALA	CZĘSTOTLIWOŚĆ WYSTĄPIENIA ZDARZENIA
Zdarzenie niemal pewne	4	zdarzenie występuje co najmniej raz w tygodniu
Zdarzenie wysoce prawdopodobne	3	zdarzenie występuje co najmniej raz w miesiącu
Zdarzenie mało prawdopodobne	2	zdarzenie występuje co najmniej raz na kwartał
Zdarzenie nieprawdopodobne	1	zdarzenie nie występuje lub występuje raz w roku

6. Organizacja identyfikuje skutek wystąpienia zdarzenia w organizacji zgodnie z poniższą skalą:

SKUTEK	SKALA	OPIS NASTĘPSTW

zdarzenie wywołuje katastrofalny skutek	4	• strata finansowa powyżej 100.000 zł dla organizacji, • strata finansowa dla osoby fizycznej, której przetwarzanie dotyczy na tyle katastrofalna w skutkach, że powoduje utratę podstawowych potrzeb jak poczucie bezpieczeństwa, • strata osobista dla osoby fizycznej, której

SKUTEK	SKALA	OPIS NASTĘPSTW
		przetwarzanie dotyczy na tyle katastrofalna w skutkach, że powoduje utratę uznania (dyskryminacja, kradzież tożsamości, naruszenie dobrego imienia), • kara finansowa nałożona przez organ nadzorczy wysokości 100.000 zł, • zakaz przetwarzania danych nałożony decyzją administracyjną przez organ nadzorczy, • strata wizerunkowa organizacji – brak zaufania ze strony osób, które organizacja obsługuje w ramach wykonywanych zadań publicznych, • orzeczenie wyroku skazującego w zakresie przetwarzania danych przez organizację.
zdarzenie wywołuje bardzo znaczący skutek	3	• strata finansowa powyżej 50.000 zł dla organizacji, • strata finansowa dla osoby fizycznej, której przetwarzanie dotyczy na tyle znacząca w skutkach, że powoduje utratę podstawowych potrzeb jak poczucie bezpieczeństwa, • strata osobista dla osoby fizycznej, której przetwarzanie dotyczy na tyle znacząca w skutkach, że powoduje utratę uznania (dyskryminacja, kradzież tożsamości, naruszenie dobrego imienia), • kara finansowa nałożona przez organ nadzorczy powyżej 50.000 zł, • zakaz przetwarzania danych nałożony decyzją administracyjną przez organ nadzorczy, • strata wizerunkowa organizacji – brak zaufania ze strony osób, które organizacja obsługuje w ramach wykonywanych zadań publicznych.

zdarzenie wywołuje znaczący skutek	2	• strata finansowa powyżej 3000 zł dla organizacji, • strata finansowa dla osoby fizycznej, której przetwarzanie dotyczy na tyle znacząca w skutkach, że powoduje utratę
SKUTEK	**SKALA**	**OPIS NASTĘPSTW**
		podstawowych potrzeb jak poczucie bezpieczeństwa, • strata osobista dla osoby fizycznej, której przetwarzanie dotyczy na tyle znacząca w skutkach, że powoduje utratę uznania (dyskryminacja, kradzież tożsamości, naruszenie dobrego imienia), • kara finansowa nałożona przez organ nadzorczy powyżej 3000 zł, • zakaz przetwarzania danych nałożony decyzją administracyjną przez organ nadzorczy, • strata wizerunkowa organizacji – brak zaufania ze strony osób, które organizacja obsługuje w ramach wykonywanych zadań publicznych.
zdarzenie wywołuje niewielki skutek	1	• strata finansowa poniżej 3000 zł dla organizacji, • strata finansowa dla osoby fizycznej, której przetwarzanie dotyczy wywołuje niewielki skutek, • strata osobista dla osoby fizycznej, której przetwarzanie wywołuje niewielki skutek, • organ nadzorczy daje upomnienie i wzywa do naprawienia braków formalnych (przy założeniu, że organizacja wypełnia wskazania organu nadzorczego), • skutek niepowodujący utraty zaufania ze strony osób fizycznych, względem których jednostka wykonuje zadania publiczne.

zdarzenie nie powoduje skutku (nie występuje)	0	• nie ma straty finansowej, • po stronie osoby fizycznej, której przetwarzanie dotyczy nie występuje ani szkoda o charakterze majątkowym, ani osobistym, • zaufanie osób, które organizacja obsługuje w ramach wykonywanych zadań publicznych nie doznaje żadnego uszczerbku.

8. Dokonanie analizy ryzyka

1. Organizacja wykorzystuje następujący wzór analizy ryzyka w zakresie wykonywania:
   1) Analizy Ryzyka Ogólnego,
   2) Oceny Skutków Dla Przetwarzania Danych (DPIA).

WZÓR ANALIZY RYZYKA:

R = P x S

WARTOŚĆ	OPIS	ZAKRES
R	poziom wyliczanego ryzyka	
P	wartość przypisana prawdopodobieństwu materializacji zagrożenia niezrealizowania założonych celów przez organizację	1 - zdarzenie nieprawdopodobne, 2 - zdarzenie mało prawdopodobne,3 - zdarzenie wysoce prawdopodobne, 4 - zdarzenie niemal pewne.
S	Skutki zdarzenia	0 – zdarzenie nie powoduje skutku (nie występuje), 1 – zdarzenie wywołuje niewielki skutek, 2 – zdarzenie wywołuje znaczący skutek,3 – zdarzenie wywołuje bardzo znaczący skutek, 4 - zdarzenie wywołuje katastrofalny skutek.

2. Organizacja przyjmuje następujący zakres macierzy:

			SKUTEK				
			0	**1**	**2**	**3**	**4**
	Zdarzenie nieprawdopodobne	**1**	**0**	**1**	**2**	**3**	**4**
	Zdarzenie mało prawdopodobne	**2**	**0**	**2**	**4**	**6**	**8**

PRAWDOPODOBIEŃSTWO	Zdarzenie wysoce prawdopodobne	3	0	3	6	9	12
	Zdarzenie niemal pewne	4	0	4	8	12	16

3. Organizacja przyjmuje klasyfikację działań w związku ze zidentyfikowanym ryzykiem w kontekście czynności przetwarzania sklasyfikowanych do Analizy Ryzyka Ogólnego:

POZIOM	SKALA WARTOŚCI	OPIS
Ryzyko NISKIE	od 0 do 4	Ryzyko akceptowane, które nie wymaga dalszego postępowania. Zaniechanie działań względem ryzyka akceptowalnego.
Ryzyko ŚREDNIE	od 6 do 9	Administrator podejmuje decyzję w zakresie: obniżanie ryzyka poprzez wdrażanie odpowiednich środków technicznych i organizacyjnych; pozostawienie ryzyka i niepodejmowanie dalszych działań; unikanie ryzyka poprzez niepodejmowanie działań, które stały się źródłem ryzyka; przeniesienie ryzyka na inny podmiot w zakresie odpowiedzialności za zarządzanie ryzykiem. Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga okresowego monitorowania
Ryzyko WYSOKIE	od 12 do 16	Poziom ryzyka nieakceptowany – wymaga bezwzględnej reakcji – cel: zredukowanie podatności

4. Organizacja przyjmuje klasyfikację działań w związku ze zidentyfikowanym ryzykiem w kontekście czynności przetwarzania sklasyfikowanych do Oceny Skutków Dla Przetwarzania Danych (DPIA):

POZIOM	SKALA WARTOŚCI	OPIS
Ryzyko NISKIE	od 0 do 4	Ryzyko akceptowane, które nie wymaga dalszego postępowania. Zaniechanie działań względem ryzyka akceptowalnego.

Ryzyko ŚREDNIE	od 6 do 9	Administrator podejmuje decyzję w zakresie: obniżanie ryzyka poprzez wdrażanie odpowiednich środków technicznych i organizacyjnych; pozostawienie ryzyka i niepodejmowanie dalszych działań; unikanie ryzyka poprzez niepodejmowanie działań, które stały się źródłem ryzyka; przeniesienie ryzyka na inny podmiot w zakresie odpowiedzialności za zarządzanie ryzykiem. Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga okresowego monitorowania
POZIOM	**SKALA WARTOŚCI**	**OPIS**
Ryzyko WYSOKIE	od 12 do 16	Wymaga bezwzględnej reakcji – cel: zredukowanie podatności Konsultacja z organem nadzorczym konieczna w momencie, kiedy Administrator nie jest w stanie zredukować ryzyka do poziomu przynajmniej średniego, mimo że przewidział wprowadzenie środków bezpieczeństwa.

9. Plan postępowania z ryzykiem wraz z wtórnym procesem szacowania ryzyka po wdrożeniu zabezpieczeń

1. Plan postepowania z ryzykiem określa:
   1) określenie grupy czynności przetwarzania, dla której zostało zidentyfikowane ryzyko,
   2) aktyw, dla którego zostało zidentyfikowane ryzyko,
   3) kategorię zagrożenia,
   4) rodzaj zagrożenia,
   5) atrybut, dla którego zidentyfikowano ryzyko,
   6) zalecenia wobec zidentyfikowanego ryzyka,
   7) komórkę organizacyjną odpowiedzialną za wprowadzenie zaleceń,
   8) termin realizacji wdrożenia zaleceń,
   9) poziom ryzyka po wprowadzeniu działań naprawczych (wtórny proces szacowania ryzyka) wraz ze skalą ryzyka po wprowadzeniu tychże działań, **10)** właściciela ryzyka.

10. Monitorowanie i przegląd ryzyka

1) Administrator deklaruje chęć utrzymania założonego poziomu bezpieczeństwa danych osobowych przetwarzanych w organizacji poprzez:
   1) przeprowadzanie nie rzadziej niż raz na rok przeglądów ryzyka,

2) przeprowadzanie nie rzadziej niż raz na 6 miesięcy przeglądów stanu bezpieczeństwa,

3) przeprowadzanie oceny skutków względem już poddanych przeglądowi w zakresie praw i wolności czynności przetwarzania, nie rzadziej, niż raz na trzy lata,

4) przeprowadzanie oceny skutków dla nowych kategorii przetwarzania czy zastosowania nowoczesnych technologii przetwarzania, przed rozpoczęciem ich przetwarzania z uwzględnieniem ochrony danych w fazie projektowania oraz domyślnej ochrony danych,

5) stosowanie procedur postępowania w przypadku wystąpienia incydentu,

6) przeprowadzanie cyklicznie szkoleń z zakresu ochrony danych osobowych,

7) ustalenie odpowiedzialności za ciągły proces minimalizacji ryzyka.

2) Administrator uwzględnia fakt, iż prowadzanie Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA) jest procesem ciągłym, a nie jednorazowym.

POLITYKA ZARZĄDZANIA INFRASTRUKTURĄ TECHNICZNĄ

1. Rejestrowanie oraz inwentaryzacja sprzętu i oprogramowania

Wszystkie aktywa mające wartość dla Szkoły w zakresie informacji są rejestrowane *(ewidencjonowane)* i inwentaryzowane w Szkole.

1.1. AKTYWA (ZASOBY INFORMACYJNE)

W Szkole zidentyfikowano podstawowe i wspierające rodzaje aktywów. Do **podstawowych aktywów** zalicza się aktywa informacyjne obejmujące: bazy danych, kartoteki, umowy, dokumentację systemową, podręczniki użytkowania, procedury operacyjne, plany ciągłości działania, licencje oprogramowania.

Katalog **aktywów wspierających** tworzą: sprzęt *(inaczej aktywa fizyczne),* oprogramowanie, sieci, ludzie, siedziby.

Do aktywów fizycznych *(sprzętu)* zalicza się: komputery stacjonarne, urządzenia przenośne m.in.: laptopy, smartfony, notebooki, urządzenia peryferyjne m.in.: serwery, drukarki, wymienne napędy dyskowe, elektroniczne nośniki danych m.in.: CD ROMy, wymienne dyski twarde, taśmy.

W grupie aktywów ***„Oprogramowanie”*** znajdują się wszystkie programy uczestniczące w operacjach przetwarzania danych tj.: systemy operacyjne, oprogramowanie narzędziowe, pakiety oprogramowania m.in.: oprogramowanie do zarządzania bazą danych, oprogramowanie do poczty elektronicznej, oprogramowanie serwera webowego, aplikacje.

W grupie aktywów ***„Sieć”*** znajdują się: media i usługi wspierające: np. sieć wewnętrzna Ethernet, specyfikacje protokołów bezprzewodowych, przekaźniki aktywne lub pasywne: np. most, router, hub, przełącznik, interfejs komunikacyjny np.: General Packet Radio Service (GPRS), adapter Ethernet.

W grupie **„siedziba”:**

- lokalizacje: środowisko zewnętrzne obejmujące lokalizacje, w których nie można zastosować środków bezpieczeństwa organizacji *(domy pracowników pracujących w zadaniowym czasie pracy),* siedziby jednostki*,* strefy rozumiane jako fizyczne obwody zabezpieczające, wydzielające część pomieszczeń w siedzibie organizacji *(biura),*
- podstawowe usługi: usługi i urządzenia telekomunikacyjne dostarczane przez operatora *(linie telefoniczne, wewnętrzne sieci telefoniczne),* usługi komunalne i techniczne *(źródła i okablowanie)* niezbędne do doprowadzenia zasilania do urządzeń informatycznych i peryferyjnych *(zasilacze niskonapięciowe, przemienniki napięcia)*, usługi i środki *(urządzenia, sterowanie)* chłodzące i oczyszczające powietrze *(klimatyzatory).*

W grupie ***„organizacja”:*** struktura organizacyjna kwalifikacje, umiejętności, doświadczenie, organizacja projektu lub systemu – obejmuje strukturę dla określonego projektu, systemu lub usługi *(projekt opracowania nowej aplikacji, projekt migracji systemu informacyjnego)*, podwykonawcy/dostawcy/producenci – organizacje, które w wyniku zawartej umowy zapewniają organizacji zasoby lub usługi *(firma konsultingowa, firma zarządzająca monitoringiem)*.

1.2. ZASADY KORZYSTANIA Z INFRASTRUKTURY INFORMATYCZNEJ

Pracodawca powierza pracownikowi do użytkowania komputer wraz z oprogramowaniem i inne aktywa informacyjne do wykonywania zadań w ramach realizacji obowiązków służbowych. Pracodawca zastrzega, że **komputer wraz z oprogramowaniem może być używany tylko do celów służbowych.**

Pracownik jest odpowiedzialny za bezpieczeństwo i legalność wykorzystywanego oprogramowania. Zabronione jest użytkowanie sprzętu komputerowego wraz z oprogramowaniem w sposób, który może stanowić zagrożenie dla innych użytkowników i ich danych. Oprogramowanie będące własnością Szkoły przeznaczone jest do użytku służbowego. Zabronione jest przekazywanie pozyskanych kluczy do oprogramowania osobom trzecim.

Na komputerach może być zainstalowane tylko legalne oprogramowanie. Zabrania się na komputerach przechowywania m.in.: prywatnego oprogramowania, gier i prywatnych treści, dokumentów, filmów, nagrań audiowizualnych.

1.3. ODPOWIEDZIALNOŚĆ ZA AKTYWA

Pracownik ponosi odpowiedzialność majątkową z tytułu naruszenia praw autorskich, z odszkodowaniem na rzecz posiadacza praw do dzieła i kosztami sądowymi włącznie.

1.4. ZWROT AKTYWÓW

W momencie zakończenia zatrudnienia, umowy lub porozumienia pracownicy i użytkownicy podmiotów zewnętrznych są zobowiązani do zwrotu wszelkich posiadanych aktywów organizacji.

W przypadku zakończenia stosunku pracy pracownicy są zobowiązani do zwrotu wszystkich wydanych wcześniej fizycznych i elektronicznych aktywów należących do organizacji.

EWIDENCJONOWANIE *(REJESTROWANIE)* AKTYWÓW

Komputery, laptopy, notebooki, oprogramowanie, drukarki, monitory, urządzenia np. skanery i inne aktywa informacyjne są ewidencjonowane w ewidencji księgowej.

Administrator prowadzi ewidencję umów o odpowiedzialności materialnej za powierzone mienie w przypadku osób korzystających z komputerów przenośnych i telefonów służbowych.

1.5. WARTOŚĆ AKTYWÓW NA POTRZEBY ANALIZY RYZYKA

Zakwalifikowanie aktywu informacyjnego jest podstawą do jego wyceny dla potrzeb analizy ryzyka. Aktywa mają przypisaną wagę w systemie odpowiadającą rozmiarowi skutku jaki może zostać spowodowany przez incydent skierowany na ten zasób Atrybuty zasobów, które należy wziąć pod uwagę to ich wartość, wrażliwość na zagrożenia oraz związane z nimi zabezpieczenia. Wysokość ryzyka aktywów jest zależna od podatności aktywa na wybrane rodzaje zagrożeń.

2. Inwentaryzacja aktywów (zasobów) informacyjnych

W Szkole inwentaryzację oprogramowania przeprowadza się w oparciu o przepisy ustawy o rachunkowości.

3. Nośniki przenośne

Dane przechowywane są na nośnikach przenośnych jedynie w przypadkach, gdy jest to konieczne, przez czas niezbędny do spełnienia celu, w jakim zostały one na nośniku zapisane. Po ustaniu czasu przechowywania zawartość nośnika podlega skasowaniu przy użyciu narzędzi zaakceptowanych do użycia w Szkole, a w przypadku nośników optycznych stosuje się niszczenie w niszczarkach umożliwiających niszczenie tego typu nośników.

Korzystanie z nośników przenośnych dozwolone jest tylko po ich uprzednim zabezpieczeniu poprzez szyfrowanie. Ze względu na ochronę antywirusową wymaga się, aby użytkownicy korzystali wyłącznie z nośników dystrybuowanych przez jednostkę. Korzystanie z własnych nośników bez zgody dyrektora Szkoły jest zabronione.

4. Poczta elektroniczna

Poczta elektroniczna jest narzędziem służącym do wymiany służbowych informacji wewnątrz jednostki oraz prowadzenia korespondencji z podmiotami zewnętrznymi. Użytkownicy systemu poczty elektronicznej zobowiązani są do przestrzegania następujących zasad:

1) przesyłanie informacji za pośrednictwem poczty elektronicznej odbywa się zgodnie z uprawnieniami adresatów do korzystania z określonego typu danych,
2) w przypadku przesyłania informacji prawnie chronionych wewnątrz organizacji bądź informacje poza nią należy stosować rozwiązania kryptograficzne,
3) jeżeli istotne jest potwierdzenie otrzymania przez adresata przesyłki użytkownik winien skorzystać, o ile jest to technicznie możliwe, z opcji systemu poczty elektronicznej informującej o dostarczeniu i otwarciu dokumentu.

5. Tworzenie i przechowywanie kopii awaryjnych

Kopie zapasowe są podstawowym zabezpieczeniem dostępności przechowywanych w systemie informatycznym danych. Informacje przechowywane na serwerach i kluczowych stacjach roboczych muszą być zabezpieczane- dotyczy to również oprogramowania, w szczególności, gdy ponowna instalacja i konfiguracja jest czasochłonna.

Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania została zawarta w dokumencie *Polityka Tworzenia Kopii Zapasowych,* stanowiącym załącznik nr 4 do Polityki Bezpieczeństwa Informacji Szkoły.

6. Przeglądy i konserwacja systemów

Za przeglądy i konserwacje sprzętu komputerowego, wynikające z eksploatacji, warunków zewnętrznych oraz ważności systemu dla funkcjonowania Szkoły odpowiedzialny jest ADO. Bieżącą konserwację i naprawę sprzętu wykonuje operator lub firmy zewnętrzne pod nadzorem operatora. Procedury wykonania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych zostały uregulowany w § 17 Polityki Ochrony Danych Osobowych w Szkole.

7. Zabezpieczenia przed kodem złośliwym

Wdrożono systemy antywirusowe działające na poszczególnych stacjach roboczych oraz skanujące zawartość poczty elektronicznej. Określono reguły bezpiecznego wykorzystania zasobów informatycznych, minimalizujące skutki szkodliwego oprogramowania. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego został uregulowany w *Polityce Profilaktyki Antywirusowej,* stanowiącej załącznik nr 6 do Polityki Bezpieczeństwa Informacji Szkoły.

8. Kontrola legalności oprogramowania

Co najmniej raz w roku ADO lub osoba przez niego upoważniona wykonuje raport o nowo zainstalowanych programach. Sprawdza czy nowo zainstalowane programy posiadają ważne licencje oprogramowania. W przypadku, kiedy nowo zainstalowane oprogramowanie nie posiada ważnej licencji, usuwa takie oprogramowanie z komputera i sporządza raport.

Co najmniej raz w roku ADO lub osoba przez niego upoważniona przeprowadza kontrolę legalności oprogramowania, z którego wykonuje raport zainstalowanego oprogramowania i sprawdza czy ilość posiadanych licencji odpowiada ilości licencji zainstalowanych.

9. Zarządzanie ciągłością działania

Szkoła dba o zapewnienie ciągłości funkcjonowania usług związanych z przetwarzaniem danych. Powyższe ma na celu zapewnienie podstaw do takiego reagowania na zakłócenia warunków normalnej działalności, aby tam, gdzie jest to możliwe, szybko przywrócić normalne warunki, a tam, gdzie to niemożliwe, przejść do zaplanowanego zastępczego sposobu wykonywania zadań. Zarządzanie ciągłością działania opiera się na analizie zagrożeń i podatności i w konsekwencji ocenie ryzyka z nimi związanych.

Szkoła dba o zapewnienie zgodności zasad postępowania z przepisami obowiązującego prawa, przyjętych uwarunkowań umownych i normatywnych oraz wypracowanych standardów. Celem takiego postępowania jest unikanie naruszania jakichkolwiek przepisów prawnych, zobowiązań wynikających z ustaw, zarządzeń lub umów oraz wymagań bezpieczeństwa.

Bystrzejowice Pierwsze, dn. .....

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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, s. 1) – dalej **RODO –** nadaję upoważnienie Pani/Panu:

…….
(imię i nazwisko)

……..
(stanowisko)

do przetwarzania danych osobowych w celu pełnionych obowiązków służbowych na zajmowanym stanowisku.

Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, ustawy z dnia 25 maja o ochronie danych osobowych, Kodeksu pracy, a także z Polityką ochrony danych osobowych Pracodawcy.

Jednocześnie upoważniam Panią/Pana do tworzenia/posiadania dla potrzeb wykonywanej pracy zestawień, ewidencji oraz rejestrów z danymi osobowymi, z zachowaniem pełnej ich ochrony przy zastosowaniu środków technicznych i organizacyjnych wdrożonych w Zespole Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz.

Upoważnienie i polecenia wygasają z chwilą ustania zatrudnienia lub odwołania upoważnienia. Jednocześnie informuję, że zobowiązana/y jest Pani/Pan do zachowania w tajemnicy powyższych informacji, w szczególności w zakresie danych osobowych i sposobu ich zabezpieczania, również po odwołaniu upoważnienia, a także po ustaniu zatrudnienia.

……

podpis osoby uprawnionej do nadania

upoważnienia

Załącznik nr 1
do Polityka Postępowania z Incydentami
oraz w sytuacji naruszenia ochrony danych osobowych

ZGŁOSZENIE NARUSZENIA OCHRONY

DANYCH OSOBOWYCH

1. Data ……. Godzina …….
2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane w związku z naruszeniem (imię i nazwisko, stanowisko służbowe):

   ……

   …….
3. Lokalizacja zdarzenia (nr pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):

   ……

   ……
4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu (*opisywać charakter incydentu/naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie*):

   ……

   ……..

   ……

…….
Data i podpis osoby zgłaszającej naruszenie

…….
Data i podpis bezpośredniego przełożonego

…….
Data i podpis Inspektora Ochrony Danych Osobowych

Załącznik nr 2
do Polityki Postępowania z Incydentami
oraz w sytuacji naruszenia ochrony danych osobowych

RAPORT Z NARUSZENIA OCHRONY DANYCH

1. Data ……. Godzina …….
2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię i nazwisko, stanowisko służbowe):

   ……

   …….
3. Lokalizacja zdarzenia (nr pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):

   ……

   ……..
4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:

   ……

   ……..
5. Podjęte działania:

   ……

   ……
6. Wstępna ocena przyczyn wystąpienia naruszenia:

   ……

   ……
7. Postępowanie wyjaśniające i naprawcze:

   ……

   ……

……. …….

podpis pracownika podpis Inspektora Ochrony Danych

Załącznik nr 3 do Polityki Postępowania z Incydentami oraz w sytuacji naruszenia ochrony danych osobowych

REJESTR INCYDENTÓW

L.P.	OPIS INCYDENTU	OSOBA ZGŁASZAJĄCA	DATA ZGŁOSZENIA	CZY ZAKOŃCZONO POSTĘPOWANIE WYJAŚNIAJĄCE	OSOBA ODPOWIEDZIALNA ZA REALIZACJĘ	PRZYCZYNA INCYDENTU	PODJĘTE DZIAŁANIA	UWAGI	PODPIS IOD

Załącznik Nr 1 do Polityki ochrony danych osobowych w Zespole Szkól w Bystrzejowicach Pierwszych im. Heleny Babisz

Wykaz budynków i pomieszczeń tworzących obszar, w których przetwarzane są dane osobowe w Zespole Szkól w Bystrzejowicach Pierwszych im. Heleny Babisz

1. Wykaz budynków

Dane osobowe przetwarzane są w następującym budynku pod adresem: Bystrzejowice Pierwsze 89, 21-050 Piaski

2. Wykaz pomieszczeń

Lp.	Numer pomieszczenia (przeznaczenie)	Lokalizacja	Osoby pracujące w pomieszczeniu /stanowiska + liczba osób/	Zabezpieczenie pomieszczenia
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

.....

(podpis)

Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe

1. Pracownicy Zespołu Szkól w Bystrzejowicach Pierwszych im. Heleny Babisz odpowiadają za należyte zabezpieczenie fizyczne zasobów danych osobowych na zajmowanych stanowiskach pracy.

2. Inspektor ochrony danych zobowiązany jest przeprowadzać bezpośrednią kontrolę stanu zabezpieczeń fizycznych procesów przetwarzania danych osobowych oraz zgłaszać dyrektorowi Zespołu uwagi lub propozycje kontroli.

3. Obszarem, w którym przetwarzane są dane osobowe, jest Zespól Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz, pod adresem: Bystrzejowice Pierwsze 89, 21-050 Piaski

4. Inspektor ochrony danych (IOD) jest odpowiedzialny za prowadzenie i uaktualnianie wykazu pomieszczeń, w których przetwarzane są dane osobowe.

5. Przebywanie osób nieuprawnionych do dostępu do danych osobowych w pomieszczeniach, o których mowa w pkt 4, jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych lub za zgodą dyrektora Szkoły.

6. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do przestrzegania zasad dotyczących wprowadzania osób trzecich do obszaru przetwarzania danych osobowych, o którym mowa w ust. 3. Ruch osób z zewnątrz w wymienionym obszarze powinien odbywać się pod kontrolą osób upoważnionych.

7. Budynki lub pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.

8. Budynek i pomieszczenia Zespołu Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz posiadają następujące zabezpieczenia:

1) Zamki antywłamaniowe w każdych wejściowych drzwiach;

2) System alarmowy z kodem dla każdej upoważnionej osoby

Ochrona danych przetwarzanych na urządzeniach przenośnych

1. W przypadku przetwarzania danych osobowych na urządzeniach przenośnych lub dokumentach papierowych poza obszarem wymienionym w pkt 3 - *Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe*, należy bezwzględnie chronić te dane przed dostępem do nich osób nieupoważnionych.

2. Zasady ochrony komputerów przenośnych, na których przetwarzane są dane osobowe, określa *„Polityka kontroli dostępu do informacji”*.

3. Pracownicy Zespołu Szkól w Bystrzejowicach Pierwszych im. Heleny Babisz na bieżąco monitorują ochronę zasobów danych osobowych oraz informują o zmianie uprawnień do przetwarzania danych osobowych IOD.

4. Dyrektor Zespołu Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz na bieżąco informuje IOD o:

1) ustaniu zatrudnienia osoby w Szkole, celem kontroli aktywności jego kont w systemie informatycznym,
2) przeniesieniu pracownika na inne stanowisko pracy, celem kontroli jego uprawnień do dostępu do danych osobowych.

5. IOD ustala szczegółowe zakresy informacji oraz formę i tryb ich przekazywania.

6. Każda zmiana informacji w zakresie ujętym w pkt 2–3 wymaga bieżącej aktualizacji przez osoby wskazane w wymienionych punktach.

Załącznik Nr 7 do Polityki ochrony danych osobowych w Zespole Szkól w Bystrzejowicach Pierwszych im. Heleny Babisz

Ewidencja podmiotów przetwarzających, którym powierzono przetwarzanie danych

L.p.	Nazwa podmiotu przetwarzającego, któremu powierzono przetworzenie danych	Podstawa prawna powierzenia przetwarzania/ Nr umowy	Data powierzenia	Zakres powierzenia	Uwagi
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					

Załącznik Nr 8

do Polityki ochrony danych osobowych w Zespole Szkól w Bystrzejowicach Pierwszych im. Heleny Babisz

ZASADY PROWADZENIA SZKOLEŃ Z ZAKRESU OCHRONY DANYCH OSOBOWYCH W ZESPOLE SZKÓL W BYSTRZEJOWICACH PIERWSZYCH IM. HELENY BABISZ

1. Każdy użytkownik systemu uczestniczący w operacjach przetwarzania danych osobowych musi odbyć szkolenie z zakresu ochrony danych osobowych.

2. Cel prowadzenia szkoleń:
1) zapoznanie pracowników z obowiązującymi przepisami dotyczącymi ochrony danych osobowych,
2) zapoznanie z obowiązującymi wewnątrz Szkoły przepisami, politykami, procedurami, instrukcjami,
3) budowanie świadomości użytkowników,
4) postępowanie zgodnie z przyjętymi zasadami,
5) uświadomienie skali zagrożeń,
6) podniesienie kompetencji użytkowników.

3. Formy szkolenia:
1) przeprowadzanie szkoleń przez IOD,
2) przeprowadzanie szkoleń przez osoby funkcyjne,
3) samokształcenie na podstawie udostępnionych materiałów,
4) przeprowadzenie szkoleń przez wyspecjalizowany podmiot zewnętrzny.

Etapy szkolenia użytkowników:
1) przed wydaniem upoważnienia do przetwarzania danych (dopuszczeniem do przetwarzania), szkolenia wstępne prowadzone są przez Inspektora Ochrony Danych,
2) okresowe szkolenia, co najmniej raz na dwa lata organizowane są przez Inspektora Ochrony Danych,
3) samokształcenie przez podsyłanie przez IOD materiałów do zapoznania się przez użytkowników,
4) „doszkalanie", krótkie szkolenia w przypadku stwierdzenia niewłaściwego postępowania lub niestosowania się do obowiązujących przepisów lub regulacji wewnętrznych.

4. Każdy użytkownik systemu, użytkownik zewnętrzny, po przeszkoleniu podpisuje oświadczenie o zachowaniu w tajemnicy danych, z którymi mają styczność oraz środkach bezpieczeństwa stosowanych przy przetwarzaniu danych osobowych oraz o zapoznaniu się z przepisami i procedurami. Wzór oświadczenia stanowi **załącznik nr 5** do Polityki.

Załącznik Nr 3 do Polityki ochrony danych osobowych w Zespole Szkól w Bystrzejowicach Pierwszych im. Heleny Babisz

REJESTR CZYNNOŚCI PRZETWARZANIA

	1	2	3	4	5	6	7	8	9	10
LP.	Nazwa czynności przetwarzania	Cel przetwarzania	Kategorie osób	Kategorie danych	Planowany termin usunięcia kategorii danych (jeżeli jest to możliwe)	Nazwa współadministratora i dane kontaktowe (jeśli dotyczy)	Nazwa podmiotu przetwarzającego i dane kontaktowe (jeśli dotyczy)	Kategorie odbiorców (innych niż podmioť przetwarzający)	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 (jeżeli jest to możliwe)	Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)
	Art. 30 ust. 1	Art. 30 ust. 1 pkt b	Art. 30 ust. 1 pkt c	Art. 30 ust. 1 pkt c	Art. 30 ust. 1 pkt f	Art. 30 ust. 1 pkt a	Art. 30 ust. 1 pkt d	Art. 30 ust. 1 pkt d	Art. 30 ust. 1 pkt g	Art.30ust.1pkte
1.	Rekrutacja pracowników obsługi, administracyjnych oraz nauczycieli	Rekrutacja pracowników	Kandydaci do pracy	Dane identyfikacyjne, dane adresowe, dane o wykształceniu, stażu pracy, uprawnieniach zawodowych.	Po zakończeniu procesu rekrutacyjnego	Nie dotyczy	Nie dotyczy	Dane nie są przekazywane innym podmiotom	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla osób upoważnionych.	Nie dotyczy

2.	Prowadzenie rejestru pracowników, akt pracowniczych i ewidencji czasu ich pracy	Prowadzenie ewidencji pracowników zgodnie z Kodeksem Pracy	Pracownicy pomocniczy (sprzątaczki, pracownicy gospodarczy), administracyjni, nauczyciele	Dane identyfikacyjne, dane adresowe, dane o wykształceniu, przebiegu pracy, absencji (urlopy, zwolnienia lekarskie, rehabilitacyjne, szkoleniowe i inne), dane o zakresie obowiązków, stawce wynagrodzenia, karach i nagrodach oraz inne dane wymagane zgodnie z Kodeksem Pracy	50 lat [art. 51u ust 1 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2018 r., poz. 217 tj.)]	Nie dotyczy	Nie dotyczy	ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania antywirusowego.	Nie dotyczy

3.	Zgłoszenie pracowników i członków ich rodzin do ZUS, ich aktualizacja i przekazywanie danych o zwolnieniach.	Zgłoszenia pracownika i członków jego rodziny do ZUS, ich aktualizacja oraz przekazywanie informacji o zwolnieniach.	Pracownicy pomocniczy (sprzątaczki, pracownicy gospodarczy), administracyjni, nauczyciele	Dane identyfikacyjne, dane adresowe, dane o Oddziale NFZ oraz inne dane wymagane w formularzu zgłoszenia ZUS ZUA - zgłoszenie, ZUS IUA - zmiana danych, ZUS ZWUA - wyrejestrowanie, ZUS ZCNA -zgłoszenie członka rodziny, ZAS - wniosek o ustalenie okresu zasiłkowego, OL-2 - wniosek o kontrolę zaświadczenia lekarskiego, Z15a - zgłoszenie opieki nad dzieckiem, Z15B - zgłoszenie opieki nad innym członkiem rodziny	50 lat [art. 125a ust 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U z 2017 r., poz.1383)]	Nie dotyczy	Nie dotyczy	ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania antywirusowego.	Nie dotyczy

4.	Prowadzenie rozliczeń z pracownikami, wypłata wynagrodzeń naliczanie obciążeń oraz naliczanie składek do ZUS	Prowadzenie rozliczeń z pracownikami, naliczanie potraceń, obliczanie składek ZUS	Pracownicy pomocniczy (sprzątaczki, pracownicy gospodarczy), administracyjni, nauczyciele	Dane identyfikacyjne, dane adresowe, dane kadrowe (wysługa lat pracy, stawka wynagrodzeń), dane o czasie pracy, przyznanych nagrodach, potraceniach (składki związkowe, zajęcia komornicze itp.) numery kont dla przelewów bankowych pracownika	50 lat [art. 125a ust 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z2017 r., poz.1383)]	Nie dotyczy	Nie dotyczy	Banki, urzędy skarbowe, ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe,	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, system antywirusowy.	Nie dotyczy
5.	Rekrutacja uczniów/ dzieci	Rekrutacja dzieci do Przedszkola i Szkoły Podstawowej w Zespole Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz	Kandydaci, rodzice, opiekunowie prawni	Imię, nazwisko, data urodzenia oraz numer PESEL kandydata, a w przypadku braku numeru PESEL - serię i numer paszportu lub innego dokumentu potwierdzającego tożsamość; adres´ poczty elektronicznej i numery telefonów rodziców/opiekunów kandydata, oświadczenie o miejscu zamieszkania rodziców kandydata i kandydata, oświadczenie o wielodzietności rodziny kandydata ,orzeczenie o potrzebie kształcenia specjalnego wydane ze względu na niepełnosprawność,´ orzeczenie o niepełnosprawności lub o stopniu niepełnosprawności lub orzeczenie równoważne, prawomocny wyrok sądu rodzinnego orzekający rozwód lub separację lub akt zgonu oraz oświadczenie o samotnym wychowywaniu dziecka oraz	1 rok [art. 160 ust. 2 ustawy z 14 grudnia 2016 r. Prawo oświatowe (Dz.U. z 2017 r., poz. 59)]	Nie dotyczy	Nie dotyczy	Dane nie są przekazywane podmiotom	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla osób upoważnionych, instalacja oprogramowania antywirusowego.	Nie dotyczy

				niewychowywaniu żadnego dziecka wspólnie z jego rodzicem, dokument poświadczający objecie dziecka pieczą zastępczą, oświadczenie o dochodzie ną osobę w rodzinie kandydatą						

6.	Ewidencja uczniów	Prowadzenie ewidencji dzieci	Dzieci	Dane identyfikacyjne dziecka (imię, nazwisko, data i miejsce urodzenia, numer PESEL), adres zamieszkania dziecka, dane o rodzicach/opiekunach prawnych (imię, nazwisko, adres zamieszkania – jeżeli są różne od adresu zamieszkania dziecka), data rozpoczęcia obowiązku przedszkolnego	10 lat	Nie dotyczy	Nie dotyczy	Dane są przekazywane do Systemu Informacji Oświatowej na podstawie art. 14 Ustawy z dnia 15 kwietnia 2011 r. o Systemie Informacji Oświatowej Dz. U. 2017, poz. 2159)	Ściśle kontrolowany dostęp do danych - dostęp tylko dla uprawnionych, zarejestrowanych użytkowników. Komputery używane do dostępu do danych zabezpieczono przed atakami z sieci zewnętrznej systemem antywirusowym. Serwer i dostęp do baz danych zabezpieczony jest przez dostawcę usługi wdrożeniem środków ochrony fizycznej i logicznej, poprzez zastosowanie systemu antywirusowego.	Nie dotyczy
7.	Oświadczenie o zapoznaniu się z ochroną danych osobowych	Prowadzenie ewidencji upoważnień zgodnie z RODO i Polityką Ochrony Danych Osobowych	Imię i nazwisko	Dane identyfikacyjne	Po ustaniu stosunku pracy	Nie dotyczy	Nie dotyczy	Dane nie są przekazywane innym podmiotom	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla osób upoważnionych.	Nie dotyczy
8.	Ewidencja upoważnień	Prowadzenie ewidencji upoważnień zgodnie z RODO	Imię i nazwisko, stanowisko, miejsce pracy, numer PESEL, data urodzenia.	Dane identyfikacyjne.	Po ustaniu stosunku pracy.	Nie dotyczy	Nie dotyczy	Dane nie są przekazywane innym podmiotom	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla osób upoważnionych.	Nie dotyczy

Załącznik Nr 6
do Polityki ochrony danych osobowych w Zespole Szkól w Bystrzejowicach Pierwszych im. Heleny Babisz

Oświadczenie pracownika o poufności

Oświadczam, iż zapoznano mnie z przepisami dotyczących ochrony danych osobowych, w szczególności 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 ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz.1000)

Zobowiązuję się do:

- zachowania w tajemnicy danych osobowych, do których mam lub będę miał/a dostęp w trakcie wykonywania czynności zleconych przez Pracodawcę w fizycznym obszarze przetwarzania, których Administratorem Danych Osobowych jest Zespół Szkół w Bystrzejowicach Pierwszych im. Heleny Babisz.
- zgłaszania sytuacji (incydentów) naruszenia zasad ochrony danych osobowych bezpośredniemu przełożonemu.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższym zobowiązaniem, może być uznane za naruszenie przepisów karnych ww. Rozporządzenia Parlamentu Europejskiego i Rady (UE) o Ochronie Danych Osobowych.

……..

(data i czytelny podpis pracownika)

Załącznik Nr 6 do Polityki ochrony danych osobowych w Zespole Szkól w Bystrzejowicach Pierwszych im. Heleny Babisz

Ewidencja osób upoważnionych do przetwarzania danych osobowych

L.p.	Imię i nazwisko	Komórka organizacyjna	Stanowisko	Data nadania upoważnienia	Data ustania upoważnienia	Numer upoważnienia	Uwagi
1							
2							
3							
4							
5							
6							
7							