Nazwa jednostki organizacyjnej	**PUBLICZNA SZKOŁA PODSTAWOWA W KOPCIACH**
Adres	Kopcie 21, 07-110 Grębków
Tytuł dokumentu	**POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH**
	Dokument zawiera: **opis technicznych i organizacyjnych środków bezpieczeństwa przetwarzania danych osobowych** Dokument jest załącznikiem do Rejestru Czynności Przetwarzania Danych Osobowych wprowadzonego Zarządzeniem Nr …… Dyrektora Publicznej Szkoły Podstawowej w Kopciach z dn. ……..……
Opracował	Inspektor Ochrony Danych / TBD MAZOWSZE Sp. z o.o.
Zatwierdził	Dyrektor Publicznej Szkoły Podstawowej w Kopciach Dorota Czajkowska …….. (podpis)
Wydanie	Wydanie I
Osoba odpowiedzialna	Inspektor Ochrony Danych - Marek Daniel
Miejscowość	Kopcie
Data dokumentu	……..……
Data obowiązywania	bezterminowo

Historia zmian dokumentu

Wydanie	**Data wydania**	**Administrator Danych**	**Osoba wprowadzająca zmiany**	**Komentarz** (powód wydania, zakres zmian)
I	……..……	Dorota Czajkowska	Marek Daniel	Dokument wprowadzony wg wymagań RODO

SPIS TREŚCI:

1 POLITYKA BEZPIECZEŃSTWA PUBLICZNEJ SZKOŁY PODSTAWOWEJ W KOPCIACH

Dyrektor Dorota Czajkowska reprezentująca Publiczną Szkołę Podstawową w Kopciach przyjęła poniższą Politykę Bezpieczeństwa przetwarzania danych osobowych w celu zaspokojenia potrzeb i oczekiwań społeczności lokalnej, podmiotów współpracujących oraz innych zainteresowanych stron, związanych z zachowaniem gwarancji bezpieczeństwa i poufności przetwarzanych informacji.

1. Jesteśmy świadomi ważności informacji przetwarzanych w Publicznej Szkole Podstawowej w Kopciach, i będziemy postępować tak, aby zapewnić ich bezpieczeństwo.
2. Zobowiązujemy się do spełnienia wymagań prawnych związanych z bezpieczeństwem informacji, szczególnie w zakresie przepisów prawnych dotyczących ochrony danych osobowych.
3. Zakresem ochrony objęto wszelkie informacje przetwarzane w Publicznej Szkole Podstawowej w Kopciach, w każdej formie i w każdym z miejsc działania jednostki, ze szczególnym uwzględnieniem danych osobowych.
4. Za bezpieczeństwo informacji w Publicznej Szkole Podstawowej w Kopciach odpowiada każdy właściciel zasobów na swoim stanowisku pracy.
5. Zapewnienie bezpieczeństwa przetwarzania danych osobowych koordynuje Inspektor Ochrony Danych.
6. Na podstawie niniejszej Polityki zostały sformułowane poszczególne cele w zakresie bezpieczeństwa informacji, które są realizowane poprzez odpowiednie polityki i inne zabezpieczenia organizacyjno-techniczne, obejmujące w szczególności:
   6.1. zapewnienie wykształcenia i świadomości pracowników w zakresie bezpieczeństwa informacji a w szczególności ochrony danych osobowych,
   6.2. zapewnienie ciągłości działania Publicznej Szkoły Podstawowej w Kopciach,
   6.3. zakomunikowanie pracownikom konsekwencji, w tym dyscyplinarnych, w przypadku naruszenia bezpieczeństwa informacji,
   6.4. raportowanie incydentów związanych z bezpieczeństwem informacji,
   6.5. w Publicznej Szkole Podstawowej w Kopciach dokonano szacowania ryzyka zgodnie z przyjętą metodą i kryteriami akceptacji ryzyka, opisanymi w raporcie z analizy ryzyka, a następnie wdrożono w stosunku do zidentyfikowanych ryzyk stosowne zabezpieczenia, zgodnie z rekomendacjami.
7. Obowiązkiem pracowników Publicznej Szkoły Podstawowej w Kopciach jest przestrzeganie zasad postępowania zawartych w RODO oraz udokumentowanych w niniejszej Polityce i w opisie technicznych i organizacyjnych środków bezpieczeństwa przetwarzania danych osobowych.
8. Pracownicy Publicznej Szkoły Podstawowej w Kopciach w ramach zdobytej wiedzy dotyczącej ochrony danych osobowych realizują zasady dotyczące ochrony oraz analizują i eliminują błędy w tym zakresie.

Niniejsza Polityka oraz pozostała dokumentacja bezpieczeństwa funkcjonująca w Publicznej Szkole Podstawowej w Kopciach została zaakceptowana przez Dyrektora oraz zakomunikowana wszystkim pracownikom, którzy zostali zobligowani do jej stosowania.

Nad przestrzeganiem Polityki czuwa Dyrektor oraz Inspektor Ochrony Danych Osobowych.

Dokument Polityki Bezpieczeństwa przetwarzania danych osobowych został zakomunikowany wszystkim pracownikom Publicznej Szkoły Podstawowej w Kopciach oraz zainteresowanym stronom zewnętrznym.

2 DEKLARACJA STOSOWANIA

Administrator Danych deklaruje, że przetwarzanie danych osobowych w Publicznej Szkole Podstawowej w Kopciach jest zgodne z mającymi zastosowanie wymaganiami prawnymi.

Deklaracja ta opiera się w szczególności na zapewnieniu, że dane osobowe są:

1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,
2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i przetwarzane w sposób zgodny z tymi celami,
3) adekwatne, stosowne oraz ograniczone do tego co niezbędne do celów, w których są przetwarzane,
4) prawidłowe i w razie potrzeby uaktualniane,
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
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.

3 DEFINICJE

Definicje pojęć używanych w dokumencie:

1. **Rozporządzenie RODO/GDPR** – Rozporządzenie 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 (GDPR– General Data Protection Regulation).
2. **Ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.
3. **Dane osobowe** –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, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
4. **Przetwarzanie danych** – 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.
5. **Zbiór danych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
6. **Administrator Danych,** (AD) – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

   Tu: Administratorem Danych jest Publiczna Szkoła Podstawowa w Kopciach reprezentowana przez Dyrektora, który decyduje o celach i środkach przetwarzania danych osobowych.
7. **Pracownik** - każda osoba dopuszczona do przetwarzania danych osobowych niezależnie od formy zatrudnienia (umowa o pracę, umowa cywilnoprawna, staż, praktyka).
8. **Podmiot przetwarzający** − osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu i na polecenie Administratora Danych.
9. **Strona trzecia** – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe.
10. **Odbiorca danych** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią; organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.
11. **Zgoda osoby, której dane dotyczą –** 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.
12. **Naruszenie ochrony danych osobowych** – 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.

13. **Zabezpieczenie danych** w systemie informatycznym – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych, zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
14. **Uwierzytelnienie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
15. **Autentyczność** – właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana; autentyczność dotyczy: użytkowników, procesów, systemów i informacji.
16. **Poufność informacji** – rozumiana jest jako zapewnienie, że tylko osoby uprawnione mają dostęp do informacji.
17. **Integralność informacji** – rozumiana jest jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania.
18. **Dostępność informacji** – rozumiane jest jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne
19. **Rozliczalność** – rozumiana jest jako zapewnienie możliwości przypisania w sposób jednoznaczny zrealizowanej czynności do określonego podmiotu.
20. **Niezaprzeczalność** – braku możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie.
21. **Organ nadzorczy** – niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 RODO: **Prezes Urzędu Ochrony Danych Osobowych (PUODO)**.
22. **Kontrolujący** – osoba, o której mowa w art. 79 Ustawy
23. **Inspektor Ochrony Danych**, (IOD) – osoba powołana przez Administratora, wykonująca zadania określone w art 39 RODO.
24. **Administrator Systemów Informatycznych,** (ASI) – osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych – administrator sieci lokalnej, systemów operacyjnych, baz danych, oprogramowania dziedzinowego, narzędziowego i innych.
25. **Serwisant Systemu Dziedzinowego** – osoba fizyczna lub organizacja serwisująca systemy dziedzinowe Administratorowi Danych, niezależna od Administratora Danych, sprawująca nadzór we własnym zakresie nad prawidłowością przetwarzania danych osobowych w serwisowanym rozwiązaniu bądź systemie.
26. **Użytkownik systemu** – osoba posiadająca upoważnienie wydane przez Administratora Danych lub osobę upoważnioną przez niego i dopuszczona w zakresie w nim wskazanym, jako użytkownik do przetwarzania danych osobowych w systemie informatycznym Publicznej Szkoły Podstawowej w Kopciach.
27. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
28. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
29. **Sieć telekomunikacyjna** – sieć telekomunikacyjna w rozumieniu art. 2 pkt. 35 ustawy – Prawo telekomunikacyjne.
30. **Sieć publiczna** – publiczna sieć telekomunikacyjna w rozumieniu art. 2 pkt. 29 ustawy – Prawo telekomunikacyjne.
31. **Aplikacja** – program komputerowy wykonujący konkretne zadanie.
32. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
33. **Polityka Bezpieczeństwa** – ogólny dokument deklaracji Administratora w zakresie zobowiązań, zakresu i sposobów realizacji ochrony danych osobowych.

4 PRZEDMIOT, CEL I ZAKRES DOKUMENTU.

Niniejszy dokument zawiera opis technicznych i organizacyjnych środków bezpieczeństwa przetwarzania danych osobowych i jest załącznikiem do Rejestru Czynności Przetwarzania Danych Osobowych Publicznej Szkoły Podstawowej w Kopciach, zgodnie z art. 30 ust 1 lit g) 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 (GDPR– General Data Protection Regulation).

Celem dokumentu jest wypełnienie wymogów nałożonych przez ww. rozporządzenie (RODO/GDPR) realizacja zasad bezpieczeństwa i dostosowania postępowania niezbędnego do prawidłowego wypełniania obowiązków Administratora Danych – Publiczną Szkołę Podstawową w Kopciach w zakresie zabezpieczenia danych osobowych, przetwarzanych zarówno tradycyjnie, jak i przy pomocy systemów informatycznych.

Dokument obejmuje swoim zakresem wszystkich pracowników Publicznej Szkoły Podstawowej w Kopciach, osoby i podmioty współpracujące oraz interesantów i klientów.

5 ZAKRES ODPOWIEDZIALNOŚCI PRZY PRZETWARZANIU DANYCH OSOBOWYCH.

5.1 Administrator Danych

Administrator odpowiedzialny jest za:

1. wprowadzenie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych w organizacji danych osobowych,
2. dostarczenie niezbędnych zasobów i środków do zapewnienia przetwarzania w zgodności z przepisami
3. stosowanie się do wymagań prawnych w obszarze ochrony danych osobowych,
4. wyznaczenie i odwoływanie IOD oraz wspieranie IOD w wypełnianiu przez niego zadań,
5. włączanie IOD we wszystkie sprawy dotyczące danych osobowych, niezwłoczne informowanie IOD o wszystkich zdarzeniach dotyczących bezpieczeństwa danych osobowych (art. 38 ust 1. RODO).

5.2 Inspektor Ochrony Danych

1. Inspektor Ochrony Danych odpowiedzialny jest za wypełnianie zadań określonych w art. 39 RODO, a w szczególności:
   a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie,
   b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
   c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie ich wykonania zgodnie z art. 35 RODO,
   d) współpraca z organem nadzorczym,
   e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,
   f) na podstawie art. 38 ust 4. RODO IOD udziela odpowiedzi i wyjaśnień na pytania osób których dane dotyczą we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem przysługujących im praw,
   g) na podstawie art. 38 ust 6. RODO IOD dodatkowo może wykonywać zadania nadzorcze, doradcze, monitorujące wewnętrzne dokumenty dotyczące bezpieczeństwa; monitorowanie i konsultacje przy aktualizacji rejestru czynności przetwarzania danych osobowych oraz inne zadania mogące poprawić bezpieczeństwo danych.
2. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.
3. Status Inspektora Ochrony Danych.
   a) Administrator zapewnia, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych,
   b) Administrator wspiera IOD w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania,

c) Administrator zapewnia, by IOD nie otrzymywał instrukcji dotyczących wykonywania tych zadań. IOD bezpośrednio podlega najwyższemu kierownictwu jednostki,
d) IOD jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań,
e) IOD może wykonywać inne zadania i obowiązki. Administrator zapewnia, by takie zadania i obowiązki nie powodowały konfliktu interesów.

4. Odwołanie lub zmiana Inspektora Ochrony Danych.
   a) IOD nie może być odwołany ani karany przez administratora za należyte wypełnianie swoich zadań, nie może zostać odwołany ani karany za udzielenie określonego zalecenia dotyczącego bezpieczeństwa danych osobowych, z którym nie zgadza się Administrator,
   b) zgodnie z przepisami, jak w przypadku każdego innego pracownika czy zleceniobiorcy, IOD może zostać odwołany lub ukarany w uzasadnionych sytuacjach z przyczyn innych niż wykonywanie obowiązków IOD (np. kradzież, ciężkie naruszenie obowiązków),
   c) Administrator zawiadamia Prezesa Urzędu Ochrony Danych Osobowych o każdej zmianie danych IOD oraz o odwołaniu inspektora, w terminie 14 dni od dnia zaistnienia zmiany lub odwołania.
5. Zespół Inspektora Ochrony Danych.
   a) IOD wykonując swoje zadania może korzystać z pomocy zespołu IOD,
   b) skład zespołu IOD oraz zakresy obowiązków członków zespołu określa Inspektor w uzgodnieniu z Administratorem danych.

5.3 Administrator Systemu Informatycznego

Administrator Systemu Informatycznego odpowiedzialny jest za:

1. administrację środowiskami informatycznymi przeznaczonymi do przetwarzania danych osobowych,
2. administrację uprawnieniami nadawanymi/modyfikowanymi/odbieranymi do systemów informatycznych przetwarzających dane osobowe,
3. zapewnienie ciągłości działania systemu informatycznego i optymalizację jego wydajności,
4. instalację i konfigurację sprzętu i oprogramowania oraz jego aktualizację,
5. konfigurację i administrację oprogramowaniem systemowym i sieciowym,
6. identyfikowanie i zgłaszanie do IOD oraz ADO incydentów z obszaru ochrony danych osobowych, w zakresie obsługiwanych systemów informatycznych przetwarzających dane osobowe oraz innych zdarzeń mogących mieć wpływ na bezpieczeństwo danych osobowych,
7. zapewnienie bezpieczeństwa przechowywanych w systemie teleinformatycznym danych osobowych.

5.4 Osoby przetwarzające

Wszystkie osoby przetwarzające dane osobowe w Publicznej Szkole Podstawowej w Kopciach są odpowiedzialne za:

1. przetwarzanie danych osobowych zgodnie z posiadanym aktualnie upoważnieniem,
2. przestrzeganie zasad ochrony danych osobowych określonych w przepisach prawa oraz niniejszej Polityce bezpieczeństwa przetwarzania danych osobowych, w tym:
   a) zapoznanie się przed dopuszczeniem do przetwarzania danych z wyżej wymienionymi dokumentami,
   b) złożenie stosownego oświadczenia potwierdzającego znajomość ich treści,
   c) spełnianie wymogu wynikającego z obowiązku informacyjnego, w szczególności poinformowania osoby, której dane dotyczą,
3. uczestniczenie w obowiązkowych szkoleniach z zakresu ochrony danych osobowych,

4. bezzwłoczne zgłaszanie IOD wszelkich dostrzeżonych nieprawidłowości w przetwarzaniu danych osobowych,
5. bezzwłoczne zgłaszanie wszelkich incydentów, nieprawidłowości dostrzeżonych zagrożeń związanych z bezpieczeństwem danych osobowych, wnioskowanie do IOD o potrzebie uzupełnienia lub uaktualnienia Rejestru czynności przetwarzania danych osobowych, potrzebie dokonania zmian w procesie przetwarzania danych osobowych oraz informowanie o ustaniu celu przetwarzania tych danych,
6. niezwłoczne usunięcie / zaprzestanie przetwarzania danych osobowych w momencie ustania celu ich przetwarzania,
7. informowanie IOD o zamiarze powierzenia przetwarzania danych osobowych lub ich udostępnienia innemu podmiotowi oraz konsultowanie z IOD umowy o powierzeniu przetwarzania danych osobowych,
8. zgłaszanie wszelkich planowanych nowych czynności przetwarzania danych w celu przeprowadzenia analizy i oceny ryzyk z tym związanych i ewentualnej oceny skutków oddziaływania,
9. dołożenia szczególnej staranności podczas przetwarzania danych osobowych, aby proces przetwarzania odbywał się zgodnie z prawem, dane osobowe były merytorycznie poprawne, a ich przetwarzanie odbywało się wyłącznie w celu i zakresie, dla którego zostały zebrane,
10. identyfikowanie i zgłaszanie do IOD incydentów z zakresu ochrony danych osobowych oraz innych zdarzeń mogących mieć wpływ na bezpieczeństwo danych osobowych.

6 OPIS PRZETWARZANIA DANYCH OSOBOWYCH.

Przez bezpieczeństwo należy rozumieć stan uniemożliwiający wykorzystanie, modyfikację lub zniszczenie informacji w Publicznej Szkole Podstawowej w Kopciach przez osoby postronne lub nieupoważnione. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych rozumiane jest jako zapewnienie ich poufności, integralności i dostępności.

Kierownictwo Publicznej Szkoły Podstawowej w Kopciach deklaruje pełne zaangażowanie w zapewnieniu właściwego zarządzania bezpieczeństwem informacji i oświadcza, że zgodnie z przepisami prawa oraz wymogami wynikającymi z zawartych przez Publiczną Szkołę Podstawową w Kopciach umów, realizuje zasady oraz podejmuje działania prowadzące do zapewnienia bezpieczeństwa danych osobowych.

Przyjęte środki ochrony stosuje się do wszystkich danych osobowych przetwarzanych przez pracowników Publicznej Szkoły Podstawowej w Kopciach, zarówno w ewidencjach papierowych (kartoteki, skorowidze, księgi i inne), jak i w systemach informatycznych oraz na wszelkich nośnikach lub urządzeniach końcowych (CD, DVD, taśmy, pendrive, telefony komórkowe, tablety, komputery PC, notebooki lub równoważne). Zobowiązuje się wszystkich pracowników Publicznej Szkoły Podstawowej w Kopciach do ich przestrzegania.

Opracowanie, utrzymywanie i doskonalenie środków ochrony danych osobowych jest niezbędne dla utrzymania prawidłowego funkcjonowania Publicznej Szkoły Podstawowej w Kopciach, zapewniania realizacji zadań, utrzymania ciągłości działania oraz zgodności z wymogami prawnymi.

Kierownictwo Publicznej Szkoły Podstawowej w Kopciach sprawuje należyty nadzór nad pracownikami tak, aby zapewnić bezpieczeństwo przetwarzanych danych poprzez kształcenie i szkolenia w dziedzinie bezpieczeństwa danych osobowych.

Osoby upoważnione do przetwarzania lub przebywania w strefie przetwarzania danych osobowych przed rozpoczęciem pracy zapoznawane są przez Inspektora Ochrony Danych z zasadami przetwarzania i ochrony danych.

Szkolenie z zakresu ochrony danych osobowych organizuje się co najmniej raz w roku.

Naruszenie zasad ochrony danych osobowych przyjętych przez Publiczną Szkołę Podstawową w Kopciach jest ciężkim naruszeniem obowiązków pracowniczych. Osoby naruszające te zasady zostaną pociągnięte do odpowiedzialności służbowej, a w uzasadnionych przypadkach również do odpowiedzialności karnej.

6.1 Obszar przetwarzania danych osobowych i sieć lokalna LAN

1. Obszarem przetwarzania danych osobowych w Publicznej Szkole Podstawowej w Kopciach są pomieszczenia biurowe, w których odbywa się praca na danych osobowych, miejsca przechowywania nośników informacji zawierających dane osobowe oraz pomieszczenia, w których znajduje się sprzęt służący do ich przetwarzania zlokalizowane w budynku Publicznej Szkoły Podstawowej w Kopciach, Kopcie 21, 07-110 Grębków.
2. Pomieszczenia te zabezpieczone są przed dostępem osób trzecich.
3. Osoby nieupoważnione mogą przebywać wewnątrz obszaru przetwarzania danych osobowych jedynie w obecności osoby upoważnionej do przetwarzania tych danych osobowych.
4. Obszary przetwarzania danych są odpowiednio zabezpieczone przed skutkami pożaru, włamania, ingerencji osób postronnych.
5. Za należyte zabezpieczenie fizyczne pomieszczeń stanowiących obszar przetwarzania danych odpowiada Dyrektor.
6. Ruch sieciowy podlega automatycznej weryfikacji i kontroli pod kątem poprawności ruchu oraz wykrywania zagrożeń (w zakresie zastosowanych środków sprzętowo-programowych).

7. Dokumenty papierowe przetwarza się tylko i wyłącznie w obszarach przetwarzania danych w sposób uniemożliwiający wgląd osobom nieupoważnionym.
8. Przetwarzanie danych w systemach informatycznych odbywa się jednostanowiskowo na komputerach PC, połączonych ze sobą lokalną siecią MS Windows peer-to-peer.
9. Systemy dziedzinowe, aplikacje, bazy danych zainstalowane są na stacjach roboczych, których zasoby są udostępnione upoważnionym pracownikom poprzez mechanizmy loginów i haseł.
10. Połączenie z Internetem jest realizowane poprzez łącze ZGK Grębków 30 MB/s. Sieć wewnętrzna jest połączona z siecią Internet poprzez router MIKROTIK.
11. Segment sieci LAN dla gabinetu Dyrektora jest przygotowany do oddzielona jest poprzez router i będzie wykonany po zakończeniu inwestycji LAN/światłowód z projektu Ogólnopolska Sieć Edukacyjna.
12. Sieć Wi-Fi zrealizowana jest przez wykorzystanie dwóch punktów dostępowych zainstalowanych w gabinecie Dyrektora i pokoju nauczycielskim. Dostęp do sieci Wi-Fi zabezpieczony jest hasłem.
13. Główny punkt koncentracji lokalnej sieci komputerowej zainstalowany jest w pracowni komputerowej.

6.2 Określenie środków organizacyjnych i technicznych zastosowanych dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych

6.2.1 Środki ochrony fizycznej:

1. Budynek Publicznej Szkoły Podstawowej w Kopciach posiada dwa wejścia:
   1) wejście główne do szkoły, drzwi drewniane, wyposażone w jeden zamek zwykły,
   2) wejście do szatni, drzwi metalowe, wyposażone w w jeden zamek zwykły,
2. Budynek Publicznej Szkoły Podstawowej w Kopciach jest zabezpieczony przed pożarem za pomocą gaśnic.
3. Dane osobowe w formie dokumentów papierowych przetwarzane są w pomieszczeniach biurowych: w gabinecie Dyrektora, pokoju nauczycielskim, w bibliotece i w salach lekcyjnych.
4. Dane osobowe w formie elektronicznej przetwarzane są w pomieszczeniach: w gabinecie Dyrektora, pokoju nauczycielskim.
5. Wszystkie pomieszczenia biurowe przetwarzania danych osobowych chronione są poprzez zastosowanie drzwi drewnianych z zamkami mechanicznymi, gabinet Dyrektora posiada drzwi i okna antywłamaniowe, pracownia komputerowa posiada dodatkowo kraty z dwoma kłódkami.
6. Szafy na dokumenty z danymi osobowymi wyposażone są w zamki, klucze do nich składowane są w szafce w gabinecie Dyrektora.
7. Gospodarka kluczami do pomieszczeń:
   1) klucze wejściowe do budynku Publicznej Szkoły Podstawowej w Kopciach mają osoby wymienione w wykazie osób uprawnionych do otwarcia budynku, stanowiącego Załącznik nr 6,
   2) klucze do pokoju Dyrektora ma Dyrektor,
   3) klucze do pokoju nauczycielskiego posiada Dyrektor i woźna, woźna dozoruje zamknięcie pokoju nauczycielskiego,
   4) klucze do sal lekcyjnych znajdują się na tablicy na klucze w pokoju nauczycielskim skąd nauczyciele pobierają je i zdają,
   5) klacze zapasowe przechowywane są w szafie metalowej w gabinecie Dyrektora, do której dostęp ma Dyrektor.

6.2.2 System alarmowy

W Publicznej Szkole Podstawowej w Kopciach nie został dotąd zamontowany system alarmowy.

6.2.3 Monitoring:

W Publicznej Szkole Podstawowej w Kopciach nie został dotąd zamontowany system monitoringu wizyjnego.

6.2.4 System przeciwpożarowy

1. Budynek Publicznej Szkoły Podstawowej w Kopciach jest zabezpieczony przed pożarem za pomocą czterech gaśnic: dwie na korytarzu szkolnym, po jednej w kotłowni i w bibliotece. Hydrant zlokalizowany jest przy drodze w odległości ok 100 m.
2. W budynku Publicznej Szkoły Podstawowej w Kopciach nie został dotąd zamontowany system sygnalizacji pożarowej.

6.2.5 Dostęp fizyczny do zbiorów danych osobowych

Dostęp fizyczny do zbiorów danych osobowych mają wyłącznie uprawnieni użytkownicy, IOD (w ramach działań kontrolnych) oraz osoby sprzątające obiekt.

6.2.6 Środki sprzętowe:

1. Do likwidacji zbędnych dokumentów papierowych zastosowano niszczarkę zwykłą zainstalowaną w gabinecie Dyrektora.
2. Systemy informatyczne przetwarzające dane osobowe są zainstalowane na komputerach przyłączonych do sieci LAN.
3. Dostęp do komputerów przetwarzających dane osobowe jest chroniony poprzez hasła do systemu operacyjnego i hasła aplikacji.
4. Lokalna sieć komputerowa ma połączenie z siecią publiczną Internet w sposób zapewniający kontrolę przepływu danych pomiędzy LAN a Internetem poprzez urządzenie brzegowe MIKROTIK.
5. Dane w systemach są przetwarzane w sposób scentralizowany, nie występują rozproszone bazy danych.
6. Wszystkie komputery na których przetwarzane są dane osobowe są zabezpieczone przed utratą danych na skutek zaniku zasilania, komputery stacjonarne posiadają UPS-y podtrzymujące pracę, laptopy własną baterię wewnętrzną.

6.2.7 Środki ochrony w ramach oprogramowania systemu:

1. Konfiguracja systemów umożliwia użytkownikom dostęp do danych osobowych tylko za pośrednictwem aplikacji; zabronione jest instalowanie narzędzi programowych umożliwiających dostęp do baz danych z pominięciem aplikacji.
2. Systemy operacyjne komputerów mają zdefiniowane prawa dostępu do zasobów systemu dla ASI oraz poszczególnych użytkowników dokonujących autoryzacji poprzez identyfikatory i hasła.
3. Dostęp do systemów sieciowych jest chroniony poprzez system identyfikatorów i haseł ASI oraz użytkowników.
4. Zainstalowany program antywirusowy ESET NOD32 ANTIVIRUS (lub Kaspersky Antivirus) posiada funkcje skanera zasobów dyskowych, monitora systemu, skanera poczty elektronicznej.
5. Program antywirusowy skonfigurowano w sposób zapewniający stałą, automatyczną aktualizację narzędzia, sygnatur zagrożeń oraz szczepionek.
6. Systemy operacyjne są na bieżąco aktualizowane poprzez instalowanie Serwis Pack'ów i update'ów systemu – aktualizacje automatyczne.
7. Zabrania się użytkownikom ingerencji w konfigurację ww. środków ochrony oraz samodzielnego instalowania oprogramowania.

6.2.8 Środki ochrony w ramach narzędzi baz danych i aplikacji:

1. W bazach danych i aplikacjach skonfigurowano identyfikatory i hasła uprawnionych użytkowników,
2. Użytkownicy mają nadane identyfikatory, hasła i prawa dostępu do aplikacji w stopniu zapewniającym właściwe wykonanie pracy i jednocześnie bezpieczeństwo przetwarzania danych.
3. Nie występuje udostępnianie danych osobowych w systemach informatycznych.

6.2.9 Środki organizacyjne:

1. Na podstawie umowy outsourcingowej zawartej z firmą TBD MAZOWSZE Sp. z o.o., został wyznaczony Inspektor Ochrony Danych – Pan Marek Daniel.
2. Wszyscy pracownicy zostali zaznajomieni z zasadami bezpieczeństwa obowiązującymi w Publicznej Szkole Podstawowej w Kopciach oraz przeszkoleni z przepisów RODO.
3. Wszyscy pracownicy zostali zapoznani z informacją: kto i w jakim celu przetwarza ich dane, jaki jest okres przechowywania danych, komu są lub będą udostępniane, o prawie żądanie sprostowania danych, prawie do wniesienia skargi do Prezesa UODO oraz potwierdzili zapoznanie się z powyższą informacją.
4. Osoby upoważnione do przetwarzania danych osobowych są przed dopuszczeniem ich do przetwarzania tych danych szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych oraz procedur przetwarzania danych.
5. Osoby nieupoważnione mogą przebywać wewnątrz obszaru przetwarzania danych jedynie w obecności osoby zatrudnionej przy przetwarzaniu tych danych lub Inspektora Ochrony Danych.
6. Osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem ich do przetwarzania tych danych otrzymują upoważnienie do przetwarzania danych osobowych, którego wzór określa Załącznik nr 1 i podpisują dokument „Oświadczenie o znajomości przepisów dotyczących przetwarzania danych osobowych" zawierający zobowiązanie do zachowania danych w tajemnicy.
7. Osoby upoważnione do przebywania w obszarze przetwarzania danych osobowych, nieprzetwarzające danych (sprzątaczki, pracownicy gospodarczy, itp.) otrzymują „Upoważnienie do przebywania w obszarze przetwarzania danych osobowych", którego wzór określa Załącznik nr 2 do niniejszego dokumentu i podpisują zobowiązanie do zachowania danych w tajemnicy.
8. Publiczna Szkoła Podstawowa w Kopciach jako Administrator Danych, może powierzyć podmiotom zewnętrznym przetwarzanie danych osobowych. W pisemnej umowie zawartej pomiędzy Administratorem Danych a podmiotem zewnętrznym określony zostaje w szczególności cel i zakres powierzenia przetwarzanych danych osobowych oraz zobowiązanie do przetwarzania i zabezpieczania powierzonych danych zgodnie z przepisami prawa. Wzór umowy powierzenia stanowi Załącznik nr 4 do Polityki.
9. Za nadawanie i rejestrowanie uprawnień użytkowników w systemach przetwarzających dane osobowe odpowiedzialny jest ASI. Nadawanie i modyfikacja uprawnień pracownikom w systemach IT odbywa się na podstawie pisemnego (zgodnie z Załącznikiem nr 5) lub ustnego polecenia Dyrektora.
10. Funkcję Administratora Systemów Informatycznych Publicznej Szkoły Podstawowej w Kopciach pełni nauczyciel informatyki Monika Skwierczyńska. ASI wykonuje prace związane z konfiguracją sieci, systemów operacyjnych, programów narzędziowych, wykonywaniem kopii zapasowych oraz prace związane z konfiguracją systemów dziedzinowych, za wyjątkiem programów dziedzinowych administrowanych przez firmy zewnętrzne oraz napraw sprzęty informatycznego.
11. W Publicznej Szkole Podstawowej w Kopciach dane osobowe przetwarzane są w systemie SIO oraz w programach pakietu biurowego.
12. Podmiotami przetwarzającymi dane Publicznej Szkoły Podstawowej w Kopciach na podstawie przepisu prawa są podmioty:
    a) Centrum Informatyczne Edukacji, al. J. Ch. Szucha 25, 00-918 Warszawa, System Informacji Oświatowej (MEN) – System SIO
    b) Okręgowa Komisja Egzaminacyjna w Warszawie, Plac Europejski 3, 00-844 Warszawa - System SIO EO.
13. Każdy użytkownik systemu posiada indywidualny identyfikator oraz unikalne hasło. Hasło powinno mieć co najmniej 8 znaków oraz zawierać małe i wielkie litery, cyfry i znaki specjalne. Identyfikator nie podlega zmianom. Użytkownik musi zmieniać hasło dostępu do aplikacji nie rzadziej, niż co 30 dni.
14. ASI nadaje indywidualne identyfikatory każdemu użytkownikowi systemów i sieci, a także nadaje

użytkownikom wymagany do wykonywania pracy poziom uprawnień do zasobów systemów informatycznych.

15. Jeżeli użytkownik utracił uprawnienia dostępu do systemu (także w związku z zaprzestaniem świadczenia pracy) pracownik kadr informuje o tym ASI, który bezzwłocznie blokuje konto użytkownika w systemie. Identyfikator zablokowanego użytkownika nie może przechodzić na inną osobę. Hasła użytkownika umożliwiające dostęp do systemu informatycznego użytkownik utrzymuje w tajemnicy również po upływie terminu ich ważności. Identyfikatory nie są usuwane z systemów.
16. Hasła ASI i serwisantów systemów dziedzinowych zawierają przynajmniej 10 znaków alfanumerycznych. Restrykcje dotyczące treści hasła są takie same jak dla użytkownika.
17. Identyfikatory i hasła ASI niezbędne do zarządzania systemami zostały zabezpieczone w zapieczętowanej kopercie. Koperta przechowywana jest w szafie metalowej zamykanej na klucz w do której dostęp ma Dyrektor.
18. Hasła administratorów mogą być użyte przez osoby wskazane przez Dyrektora, wyłącznie w sytuacji awaryjnej.
19. Każdy fakt użycia haseł awaryjnych musi być odnotowany na piśmie przez Dyrektora w protokole użycia haseł - Załącznik nr 3; zapisywane są informacje: kto (imię i nazwisko), komu (imię i nazwisko), kiedy (data, godzina), w jakim celu awaryjnie udostępniono hasła. O fakcie użycia haseł powiadamiany jest Inspektor Ochrony Danych który prowadzi rejestr (zbiór protokołów) wykorzystania haseł. Po każdym awaryjnym użyciu przez osoby trzecie, hasła ASI muszą być niezwłocznie zmienione.
20. Przyjęto zasadę, że danych osobowych nie wynosi się poza obszar przetwarzania danych osobowych Publicznej Szkoły Podstawowej w Kopciach. W przypadku konieczności przekazania tych danych poza obszar przetwarzania danych osobowych, Inspektor Ochrony Danych ustala sposób zabezpieczenia ich poufności i integralności, np. zaszyfrowanie nośnika lub transport danych pod ochroną.
21. Przeznaczone do naprawy urządzenia, dyski lub inne informatyczne nośniki pozbawia się przed naprawą zapisanych danych poprzez zapisanie całości przypadkową informacją przy pomocy specjalistycznego oprogramowania, albo naprawia się je pod nadzorem ASI. Uszkodzone nośniki danych osobowych niszczy się w sposób uniemożliwiający odczytanie danych.
22. W przypadku konieczności naprawy sprzętu komputerowego poza siedzibą urzędu jest on oddawany do serwisu po wyjęciu z niego nośników zawierających dane osobowe lub po skutecznym usunięciu tych danych. W przypadku sprzętu objętego gwarancję sprzęt można przekazać do naprawy gwarancyjnej jedynie po podpisaniu umowy powierzenia przetwarzania danych osobowych.
23. W pomieszczeniach gdzie przetwarzane są dane osobowe, a w których mogą przebywać osoby postronne, monitory stanowisk komputerowych ustawiono w taki sposób, aby uniemożliwić tym osobom wgląd w dane osobowe.
24. Podczas pracy w systemie informatycznym niedozwolone jest pozostawienie bez dozoru komputera z uruchomionym programem i aktywnym użytkownikiem. Wygaszacz ekranu należy skonfigurować tak, aby włączał się po upływie maksymalnie 10 minut bezczynności, a powrót do pracy w systemie wymagał ponownego podania hasła. Przy opuszczeniu stanowiska pracy pracownik musi zablokować system lub wylogować się.

6.2.10 Pozostałe zasady bezpieczeństwa przy przetwarzaniu danych osobowych

1. Kluczowe urządzenia są podłączone do urządzeń podtrzymujących napięcie (UPS), w celu umożliwienia bezpiecznego wyłączenia systemu w przypadku awarii zasilania, oraz przełączenia źródła zasilania,
2. Serwisowanie urządzeń i sprzętu na którym przetwarzane są dane osobowe następuje w możliwie krótkim czasie od wykrycia awarii, jedynie przez osoby uprawnione,
3. Na czas naprawy uszkodzonego sprzętu Kierownictwo Publicznej Szkoły Podstawowej w Kopciach dołoży starań, aby zapewnić zastępczy sprzęt o właściwościach nie gorszych niż sprzęt

przekazany do naprawy,

4. Przetwarzane bazy danych osobowych podlegają procedurze regularnego wykonywania kopii zapasowych na wypadek utraty lub niezamierzonej modyfikacji danych oraz okresowo (w ramach możliwości technicznych ASI) procedurze przywrócenia danych z kopii w celu potwierdzenia jej przydatności.
5. Okresowo ASI monitoruje stan systemów informatycznych poprzez przeglądanie i analizę logów systemowych stacji, routerów, programów oraz przeglądanie raportów programów antywirusowych i narzędziowych.
6. Nośniki informacji oraz wydruki z danymi osobowymi przechowuje się w pomieszczeniach i pojemnikach (szafy metalowe i biurowe) zamykanych na klucz.
7. Nośniki kopii zapasowych przechowuje się w szafach metalowych, w pomieszczeniach zlokalizowanych w innej części budynku niż stacje przetwarzania.
8. Usuwanie danych osobowych z dysku lub nośników zewnętrznych następuje w sposób trwały, tj.:
   a) usuniecie plików z przestrzeni dyskowej, powinno być wspierane przez dodatkowe oprogramowanie dedykowane do trwałego usuwania danych z nośników elektronicznych,
   b) kopie bezpieczeństwa usuniętych plików również podlegają powyższej procedurze; dotyczy to kopii na zewnętrznym dysku backupowym lub pendrive; kopie są utylizowane podobnie jak pliki źródłowe poprzez trwałe usunięcie lub nadpisanie dysku lub partycji z wykorzystaniem dedykowanego oprogramowania; kopie na płytach DVD, CD ulegają zniszczeniu poprzez fizyczne zniszczenie nośnika danych; jeśli na tym samym nośniku znajdowały się inne dane zostają one skopiowane na inne nośniki zewnętrzne,
   c) wydruki papierowe zawierające dane osobowe oraz zbiory osobowe przetwarzane w wersji papierowej ulegają zniszczeniu w niszczarkach dokumentów.
   d) wydruki papierowe zawierające dane osobowe pochodzące z archiwum są niszczone w niszczarkach we własnym zakresie, po uzyskaniu zgody Archiwum Państwowego.
9. Przeglądy okresowe urządzeń, na których przechowywane są dane osobowe i systemy je przetwarzające wykonywane są w odpowiednim zakresie przez ASI lub serwisanta systemu dziedzinowego w zakresie swojego systemu, w przypadku zgłaszania przez użytkownika problemów lub awarii oraz po wdrożeniu nowego systemu.
10. Zgodnie z art. 32 ust 1 pkt c i d RODO raz na 6 m-cy ASI wykonuje testowe odtwarzanie systemów z kopii według Procedury odtwarzania systemu po awarii, oraz ich testowania – Załącznik nr 12.

7 POZOSTAŁE WYMAGANIA:

7.1 Rejestr czynności

Dla wszystkich zidentyfikowanych kategorii danych osobowych, Administrator Danych przy wsparciu IOD oraz współpracy z ASI prowadzi Rejestr czynności przetwarzania danych osobowych. Rejestr czynności przetwarzania danych osobowych jest prowadzony w formie papierowej lub elektronicznej (arkusz kalkulacyjny Excel).

Na rejestr czynności przetwarzania danych osobowych składają się co najmniej następujące informacje:

1. nazwa oraz dane kontaktowe Administratora danych, współadministratorów, oraz IOD
2. liczba porządkowa,
3. nazwa czynności przetwarzania,
4. komórka organizacyjna Administratora przetwarzająca dane,
5. opis kategorii osób, których dane dotyczą,
6. cel przetwarzania danych osobowych,
7. podstawa prawna przetwarzania,
8. źródło danych osobowych,
9. opis kategorii danych osobowych,
10. systemy teleinformatyczne, w których przetwarzane są dane osobowe,
11. informacja o przetwarzaniu danych osobowych w formie papierowej,
12. planowany termin usunięcia danych osobowych,
13. ogólny opis stosowanych zabezpieczeń organizacyjnych i technicznych, odwołanie do niniejszego dokumentu,
14. informacje o podmiotach, którym powierzono przetwarzanie danych osobowych,
15. informacje o podmiotach, którym udostępniono dane osobowe,
16. informacje o przekazaniu danych osobowych do Państwa trzeciego, (gdy ma zastosowanie)

7.2 Obowiązek informacyjny

Każdorazowo, podczas zbierania danych osobowych, należy przekazać lub umożliwić osobie, której dane dotyczą informacje:

1. tożsamość/nazwę i dane kontaktowe Administratora,
2. dane kontaktowe IOD (np. adres email),
3. cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania
4. informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeśli istnieją
5. gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do Państwa trzeciego lub organizacji międzynarodowej oraz wzmiankę o stosowanych zabezpieczeniach, możliwościach uzyskania kopii tych danych lub o miejscu ich udostępnienia,
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 odbywa się na podstawie uzyskanej zgody - informacje o prawie do cofnięcia zgody na przetwarzanie danych osobowych,
9. informację o prawie do wniesienia skargi do organu nadzorczego,
10. w przypadku, gdy dane osobowe zbierane są bezpośrednio od osoby, której dane dotyczą, należy przekazać 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 konsekwencjach niepodania danych,

11. w przypadku, gdy dane osobowe pozyskiwane są w inny sposób niż od osoby, której dane dotyczą, należy przekazać osobie, której dane dotyczą informacje zawarte w pkt. 8.1. oraz uzupełnione o:
    a) kategorie przetwarzanych danych osobowych,
    b) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie również informacji czy pochodzą one ze źródeł publicznie dostępnych,
12. w przypadku, gdy planuje się dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, należy poinformować osobę, której dane dotyczą, o nowym celu przetwarzania oraz udzielić jej stosowanych informacji zawartych w niniejszym punkcie,
13. do realizacji obowiązku informacyjnego zobowiązani są wszyscy nauczyciele i pracownicy biurowi Publicznej Szkoły Podstawowej w Kopciach.

Obowiązek informacyjny realizuje się:

1. ustnie – w przypadku bezpośredniego kontaktu z osobą, której dane dotyczą lub poinformowanie, że szczegóły związane z obowiązkiem informacyjnym znajdują się na stronie internetowej wraz z podaniem adresu strony.
2. pisemnie – jako integralną część umowy lub innego dokumentu z podmiotem zewnętrznym zawierającego dane osobowe,
3. w formie elektronicznej – jako informacja w systemie teleinformatycznym przetwarzającym dane osobowe, lub jako informacja (np. w przypadku monitoringu), że szczegóły związane z obowiązkiem informacyjnym znajdują się na stronie internetowej organizacji.
4. w formie e-mail – w przypadku korespondencji e-mail.
5. podstawowe informacje mające zastosowanie w obszarze ochrony danych osobowych udostępniane są na stronie internetowej Administratora Danych.

Treść spełniająca wymagania obowiązku informacyjnego została zamieszczona w Załączniku Nr 8. do niniejszego dokumentu.

7.3 Prawa Osób – prawo dostępu

1. Prawo dostępu przysługujące osobie, której dane dotyczą. Każda osoba (która dowiedzie swoją tożsamość), której dane dotyczą jest uprawniona do uzyskania potwierdzenia, czy w Publicznej Szkole Podstawowej w Kopciach przetwarzane są jej dane osobowe.

   Na wniosek osoby, której dane dotyczą, należy przekazać informacje o:

   1) celu przetwarzania danych osobowych,
   2) kategoriach przetwarzanych danych osobowych,
   3) odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w Państwach trzecich lub organizacjach międzynarodowych oraz zabezpieczeniach wykorzystywanych w związku z tym przekazaniem
   4) planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, kryteriach tego okresu,
   5) prawie do żądania od Administratora sprostowania, usunięcia lub ograniczenia przetwarzania jej danych osobowych, oraz prawie wniesienia sprzeciwu wobec takiego przetwarzania,
   6) prawie wniesienia skargi do organu nadzorczego,
   7) źródle pozyskiwania danych osobowych, jeśli nie zostały zebrane od osoby, której dane dotyczą,

2. W przypadku wystąpienia przez osobę, które dane dotyczą o kopię danych osobowych, należy zgłosić taki fakt Administratorowi Danych oraz IOD.

3. Administrator Danych dostarcza osobie, której dane dotyczą kopię danych podlegających przetwarzaniu, **jeśli podstawą ich przetwarzania nie jest wykonywanie obowiązków publicznych.**
4. Administrator Danych podejmuje decyzję o formie, w której zostanie przekazana kopia danych oraz wysokościach opłat za wszelkie kolejne kopie.
5. Administrator Danych ma prawo odmowy przekazania kopii danych osobowych w przypadku, gdy może to wpłynąć na prawa i wolności innych osób.

7.4 Prawa Osób: do sprostowania, usunięcia, ograniczenia, przenoszenia oraz sprzeciwu wobec przetwarzania danych osobowych.

1. Prawo do sprostowania - każda osoba, której dane dotyczą ma prawo do żądania niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Osoba, której dane dotyczą ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
2. Prawo do usunięcia danych („Prawo do bycia zapomnianym") - każda osoba, której dane dotyczą, ma prawo żądania niezwłocznego usunięcia jej danych osobowych.
3. Prawo do ograniczenia przetwarzania - każda osoba, której dane dotyczą, ma prawo żądania od Administratora ograniczania przetwarzania jej danych osobowych.
4. Prawo do przenoszenia danych - osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła Administratorowi Danych oraz ma prawo przesłać te dane osobowe innemu Administratorowi Danych bez przeszkód ze strony Administratora Danych, któremu dostarczono te dane osobowe.
5. Prawo do sprzeciwu - osoba, której dane dotyczą ma prawo wnieść sprzeciw wobec przetwarzania jej danych osobowych.

Prawa osób których dane dotyczą, opisane w pkt. 2 do pkt. 5, stosuje się o ile nie są ograniczone innymi przepisami prawa.

7.5 Zasady realizacji praw osób, których dane dotyczą

1. Wnioski o realizację praw osób, których dane dotyczą kierowane są na adres: Publiczna Szkoła Podstawowa w Kopciach, Kopcie 21, 07-110 Grębków, lub na adres e-mail: iod-md@tbdsiedlce.pl.
2. W przypadku, gdy wniosek zostanie skierowany do pracownika Publicznej Szkoły Podstawowej w Kopciach należy przekazać go do IOD.
3. IOD dokonuje analizy wniosku oraz weryfikuje zasadność realizacji prawa osoby, której dane dotyczą.
4. W przypadku braku zasadności realizacji prawa, IOD zobligowany jest do niezwłocznego (nie dłużej niż 1 miesiąc) przekazania tej informacji osobie wnioskującej wraz z właściwym uzasadnieniem decyzji.
5. W przypadku pozytywnej oceny wniosku, IOD zobligowany jest do wszczęcia postępowania mającego na celu realizację prawa osoby wnioskującej. Po zakończeniu działań związanych z realizacją prawa osoby wnioskującej, IOD informuje o tym fakcie osobę wnioskującą. W przypadku, gdy czas realizacji prawa może przekroczyć 1 miesiąca IOD przekazuje osobie wnioskującej odpowiedź wraz z planowanym terminem realizacji prawa, o które wnioskowała, w terminie nie dłuższym niż 2 miesiące.
6. W sytuacji, w której realizacja prawa osoby, której dane dotyczą wymaga zaangażowania pracowników, na wniosek IOD pracownicy ci są zobligowani do wykonania zadań niezbędnych do realizacji prawa wnioskującego.

7.6 Naruszenia ochrony danych osobowych

1. Za naruszenie ochrony danych osobowych uznaje się 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. Każdy z pracowników Publicznej Szkoły Podstawowej w Kopciach w przypadku zidentyfikowania zdarzenia mogącego stanowić naruszenie ochrony danych osobowych, jest zobowiązany do niezwłocznego zgłoszenia tego zdarzenia do IOD poprzez: e-mail: iod-md@tbdsiedlce.pl lub w formie pisemnej.
3. W uzasadnionych przypadkach osoba, która zgłosiła naruszenie zobowiązana jest postępować zgodnie z wytycznymi IOD w zakresie zabezpieczenia materiału dowodowego i jeśli zajdzie taka potrzeba zaprzestania wykonywania obowiązków służbowych w celu nienaruszania materiałów dowodowych.
4. W przypadku zakwalifikowania zdarzenia jako znaczące naruszenie ochrony danych osobowych, Administrator Danych niezwłocznie zgłasza organowi nadzorczemu fakt wystąpienia zdarzenia mogącego naruszyć bezpieczeństwo danych osobowych zgodnie ze wzorem opublikowanym na stronie UODO.
5. Jeżeli istnieje małe prawdopodobieństwo, iż naruszenie ochrony danych osobowych skutkować będzie naruszeniem praw lub wolności osób fizycznych (dzięki zastosowanym zabezpieczeniom, np. szyfrowania), Administrator Danych nie jest zobligowany do zgłoszenia takiego naruszenia do organu nadzorczego.
6. W przypadku, gdy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób, których dotyczy naruszenie, należy te osoby bez zbędnej zwłoki o tym poinformować, o ile jest to technicznie możliwe.
7. Zgodnie z w art. 33 ust. 5 RODO Administrator Danych prowadzi Rejestr naruszeń ochrony danych – Załącznik nr 11.

7.7 Audyt ochrony danych

1. IOD jest zobowiązany do prowadzenia cyklicznych audytów przestrzegania zasad ochrony danych osobowych opisanych w regulacjach wewnętrznych organizacji oraz mających zastosowanie wymaganiach prawnych. Zaleca się, aby audyty ochrony danych osobowych prowadzone były co najmniej raz w roku.
2. Podczas określania zakresu audytu ochrony danych osobowych należy wziąć pod uwagę w szczególności:
   a) obszary, w których zostały zidentyfikowane naruszenia ochrony danych osobowych,
   b) rezultaty wcześniejszych audytów ochrony danych osobowych,
   c) zmiany w otoczeniu wewnętrznym i zewnętrznym organizacji,
   d) informację zwrotną od zainteresowanych stron.
3. Audytowi ochrony danych osobowych podlegają:
   a) systemy informatyczne przetwarzające dane osobowe (zgodność funkcjonalności i zabezpieczeń systemów z mającymi zastosowanie regulacjami prawnymi),
   b) zabezpieczenia fizyczne (zabezpieczenia pomieszczeń i budynków, w których przetwarzane są dane osobowe),
   c) zabezpieczenia organizacyjne (m.in. procedury komunikacji i informowania o naruszeniach, powołanie ról odpowiedzialności, aktualność wewnętrznych aktów normatywnych),
   d) bezpieczeństwo osobowe (m.in. świadomość pracowników, realizacja szkoleń wstępnych i okresowych, aktualność uprawnień w systemach teleinformatycznych),
   e) zgodność stanu faktycznego z wymaganiami mających zastosowanie aktów prawnych oraz wewnętrznych aktów normatywnych organizacji.

4. Do przeprowadzania audytu ochrony danych osobowych upoważniony jest IOD, członek zespołu IOD lub osoba przez niego wyznaczona posiadająca niezbędną wiedzę i kwalifikacje.
5. Po wykonanym audycie osoba przeprowadzająca audyt przygotowuje i przekazuje Raport z Audytu Administratorowi.
6. W przypadku wystąpienia braku zgodności z wymaganiami prawnymi lub regulacjami wewnętrznymi, IOD inicjuje adekwatne działania redukujące zidentyfikowane ryzyko lub ryzyka.

7.8 Retencja danych

1. Dane osobowe przetwarzane w Publicznej Szkole Podstawowej w Kopciach przechowywane są przez okres nie dłuższy niż jest to niezbędne.
2. Okres przechowywania danych dostosowywany jest dostosowywany do celu, w którym zostały zebrane.
3. Okres retencji może:
   a) wynikać z przepisów prawa
   b) zostać określony przez organ nadzorczy w zakresie ochrony danych osobowych,
   c) być ustalany przez komórki organizacyjne będące właścicielami przetwarzanych danych osobowych,
   d) wynikać z zapisów konkretnej umowy.
4. Wskazany przez komórkę organizacyjną okres retencji jest weryfikowany i akceptowany przez IOD.
5. Okres retencji danych osobowych odnotowany jest w Rejestrze czynności przetwarzania w stosunku do określonej kategorii i celu, w jakim dane osobowe zostały zebrane.
6. W przypadku dokumentacji w formie papierowej, za zniszczenie danych po ustaniu okresu retencji odpowiedzialny jest każdy pracownik przetwarzający te dane. Dane powinny zostać zniszczone przy użyciu niszczarki spełniającej wymagania trzeciego stopnia poufności zgodnie z normą DIN 32757. Proces ten może zostać zlecony na zewnątrz organizacji.
7. W przypadku danych osobowych przetwarzanych w systemach teleinformatycznych, każdy pracownik przetwarzający te dane jest odpowiedzialny, w miarę możliwości, za zgłoszenie potrzeby ich usunięcia do IOD. Na podstawie wniosku, IOD kontaktuje się z wszystkimi ASI w celu usunięcia danych w wersji elektronicznej.
8. Co najmniej raz w roku Dyrektor i ASI szkoły odpowiedzialni są za przeprowadzenie weryfikacji czy cel przetwarzania danych osobowych w stosunku do danych, które przetwarzają, jest nadal aktualny oraz czy nie przetwarzają danych dłużej aniżeli zostało to określone w Rejestrze czynności przetwarzania.
9. Wyniki przeglądu są przekazywane do IOD na jego wniosek.

7.9 Zgody na przetwarzanie danych osobowych

1. W każdej sytuacji, w której nie zidentyfikowano podstawy prawnej innej niż zgoda osoby, której dane dotyczą, niezbędne jest uzyskanie takiej zgody.
2. Forma wyrażenia zgody na przetwarzanie danych osobowych (np. pracownika) jest dowolna (np. treść wiadomości e-mail, wydruk, checkbox w systemie teleinformatycznym). Forma zgody powinna gwarantować możliwość potwierdzenia uzyskania takiej zgody.
3. Wyrażenie zgody na przetwarzanie danych osobowych nie może stanowić podstawy do odmowy wykonania umowy / świadczenia usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do ich wykonania.
4. Za uzyskanie zgody na przetwarzanie danych osobowych odpowiedzialny jest pracownik pozyskujący dane osobowe od osoby, której dane dotyczą.
5. Zgoda na przetwarzanie danych osobowych powinna zawierać co najmniej:
   a) tożsamość Administratora,
   b) zamierzone cele przetwarzania, dla których dane osobowe są zbierane,

c) fakt wyrażenia zgody,
d) informację o możliwości wycofania zgody.

6. Nie dopuszcza się sytuacji, w których łączy się zgody na przetwarzanie danych osobowych zbieranych dla spełnienia różnych celów. W przypadku zbierania danych osobowych dla kilku celów jednocześnie, należy uzyskać indywidualną zgodę dla każdego z celów.
7. W przypadku gdy zgoda dotyczy danych wrażliwych, konieczne jest zebranie jej w formie pisemnego oświadczenia od osoby, której dane dotyczą.
8. Osoba, której dane dotyczą ma prawo w dowolnym momencie wycofać zgodę.
9. W przypadku uzyskania wniosku o wycofanie zgody na przetwarzanie danych osobowych, każdy pracownik jest zobowiązany do powiadomienia o tym fakcie IOD, który podejmuje właściwe kroki.

ZAŁĄCZNIK NR 1. UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH (WZÓR)

Kopcie, dn. ……

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

W związku z zapewnieniem prawidłowej ochrony danych osobowych wynikających z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (RODO) upoważniam Panią / Pana: :

……..……...……
(imię i nazwisko osoby upoważnionej)

zatrudnioną (ego) w

……
(nazwa komórki organizacyjnej)

na stanowisku: ……

do wykonywania czynności przetwarzania danych osobowych na wyznaczonym stanowisku pracy, zgodnie z powierzonymi obowiązkami pracowniczymi oraz poleceniami Administratora. Równocześnie zobowiązuję Panią / Pana do zachowania w tajemnicy danych osobowych oraz sposobów ich ochrony.

…….....…..……
(podpis Dyrektora)

OŚWIADCZENIE

Ja niżej podpisana/y ……..……..
oświadczam, że zapoznałam/em się z przepisami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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, przepisami Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych oraz przepisami wewnętrznymi dotyczącymi przetwarzania danych osobowych.
Zobowiązuje się do zachowania w tajemnicy danych osobowych oraz sposobów ich ochrony, także po ustaniu zatrudnienia. W przypadku niedopełnienia obowiązków związanych z powierzonym mi przetwarzaniem danych osobowych mogę ponosić odpowiedzialność na podstawie przepisów Regulaminu pracy, Kodeksu pracy oraz ww. przepisów o ochronie danych osobowych.

……..…….
(data i podpis pracownika)

……..…….
(upoważnienie odwołano dnia)

ZAŁĄCZNIK NR 2. UPOWAŻNIENIE DO PRZEBYWANIA W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH (WZÓR)

Kopcie, dn. ……

UPOWAŻNIENIE DO PRZEBYWANIA W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH

W związku z zapewnieniem prawidłowej ochrony danych osobowych wynikających z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (RODO) upoważniam Panią / Pana:

……..……...……
(imię i nazwisko osoby upoważnionej)

do przebywania w obszarze przetwarzania danych osobowych. Równocześnie zobowiązuję Panią / Pana do zachowania w tajemnicy danych osobowych oraz sposobów ich ochrony.

……..……
(podpis Dyrektora)

OŚWIADCZENIE

Ja niżej podpisana/y ..……..……..

w związku z upoważnieniem do przebywania w obszarze przetwarzania danych osobowych zobowiązuje się zachowania w tajemnicy informacji, w tym danych osobowych, pozyskanych w trakcie realizacji obowiązków oraz informacji o sposobie ich przechowywania i zabezpieczania. Jednocześnie zobowiązuję się wykonywać swoje obowiązki nie naruszając przepisów ww. aktów prawnych.

……..……...……
(podpis osoby ubiegającej się o dostęp)

……..……..
(upoważnienie odwołano dnia)

ZAŁĄCZNIK NR 3. PROTOKÓŁ UŻYCIA HASEŁ AWARYJNYCH (WZÓR)

Kopcie, dnia.....

Protokół użycia haseł awaryjnych

Data	Godzina	Powód/cel udostępnienia haseł

Osoby obecne przy wydaniu:

1. Wydający hasła ……..… ……
   (nazwisko i imię) (podpis)

2. Pobierający hasła ……..…… ……
   (nazwisko i imię) (podpis)

ZAŁĄCZNIK NR 4. UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH (WZÓR)

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

……., z siedzibą: ……. , reprezentowaną przy niniejszej umowie przez:
1) ……
zwaną dalej Administratorem
a
Przedsiębiorstwem/Firmą ……, zarejestrowanym w ……..……. pod numerem: ……..…… prowadzonym przez ……..……..……., reprezentowanym przy niniejszej umowie przez: ……..……
zwaną dalej „Przetwarzającym"

PREAMBUŁA

W związku z zawarciem pomiędzy Stronami umowy nr …….. z dnia ……. której przedmiotem są (np. usługi informatyczne, niezbędne do administrowania siecią informatyczną) - zwaną dalej „Umową Główną", Strony postanowiły zawrzeć umowę o następującej treści (zwaną dalej „Umową"):

§ 1. Definicje pojęć używanych w niniejszej umowie:

1. Rozporządzenie (RODO) - rozporządzenie Parlamentu Europejskiego i Rady UE 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.
2. Umowa Główna - umowa dotycząca wykonywania czynności zleconych/powierzonych (np.: serwisu systemów informatycznych, księgowości, utrzymania strony www, przetwarzania w chmurze, przetwarzania danych na podstawie outsourcingu itp.) co do której niniejsza umowa powierzenia przetwarzania danych osobowych jest komplementarna.
3. Umowa – niniejsza Umowa Powierzenia Przetwarzania Danych Osobowych.
4. Podwykonawca – inny niż Przetwarzający podmiot przetwarzający dane osobowe.

§ 2. Powierzenie przetwarzania danych osobowych

1. Administrator powierza Przetwarzającemu, dane osobowe do przetwarzania na zasadach i w celu określonym w Umowie.
2. Przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą

§ 3. Zakres i cel przetwarzania danych

1. Powierzone przez Administratora dane osobowe będą przetwarzane przez Przetwarzającego wyłącznie w celu realizacji Umowy Głównej.
2. Na mocy niniejszej umowy przetwarzający będzie przetwarzał:
   („dane zwykłe" lub „szczególne kategorie danych osobowych")
   (wskazanie kategorii osób, których dane dotyczą, np. pracownicy, klienci)
   w zakresie: (należy wymienić wszystkie rodzaje danych, np. imię, nazwisko PESEL).

3. Przetwarzanie danych osobowych powierzonych Przetwarzającemu do przetwarzania będzie miało charakter ciągły i odbywać się będzie w formie elektronicznej lub papierowej poprzez wykonywanie wszystkich czynności (operacji na danych osobowych) uzasadnionych wykonywaniem lub realizacją Umowy Głównej. Zakres czynności wykonywanych na danych osobowych obejmuje: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adoptowanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, dopasowywanie, łączenie, ograniczanie, usuwanie i niszczenie, (wskazać jakie).
4. Charakter przetwarzania wynika z Umowy Głównej i określony jest rolą Przetwarzającego, jako podmiotu świadczącego usługę
5. Umowa Główna i wykonywane zgodnie z jej zapisami zlecenia będą traktowane przez Przetwarzającego, jako udokumentowane polecenia Administratora.

§ 4. Sposób wykonania Umowy

1. Przetwarzający oświadcza, że posiada zasoby infrastrukturalne, doświadczenie, wiedzę oraz wykwalifikowany personel, w zakresie umożliwiającym należyte wykonanie Umowy, w zgodzie z obowiązującymi przepisami prawa, w szczególności, że znane mu są zasady przetwarzania i zabezpieczenia danych osobowych wynikające z Rozporządzenia.
2. Przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
3. Przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
4. Przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji Umowy.
5. Przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy (o której mowa w art. 28 ust. 3 lit. b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej Umowy, zarówno w trakcie zatrudnienia, jak i po jego ustaniu.
6. Po zakończeniu obowiązywania Umowy Głównej lub w przypadku jej wcześniejszego wygaśnięcia/rozwiązania Przetwarzający zgodnie z dyspozycją Administratora zwróci lub zniszczy, w sposób i w terminie odrębnie ustalonym z Administratorem, wszelkie powierzone na podstawie Umowy dane osobowe i ich kopie, chyba że właściwe przepisy prawa krajowego lub unijnego nakazują przechowywanie tych danych osobowych. Strony postanawiają, iż w przypadku podjęcia przez Administratora decyzji o zwrocie/przekazaniu ww. danych osobowych lub ich kopii nastąpi ono w formie wcześniej uzgodnionej z Administratorem w terminie 14 dni licząc od dnia zakończenia lub wygaśnięcia/rozwiązania Umowy.
7. W miarę możliwości Przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
8. Po stwierdzeniu naruszenia ochrony powierzonych mu przez Administratora danych osobowych Przetwarzający, bez zbędnej zwłoki, jednak w miarę możliwości nie później niż w ciągu 24 godzin od wykrycia naruszenia, zgłasza je Administratorowi. Przetwarzający bez wyraźnej instrukcji Administratora nie będzie powiadamiał o naruszeniu osób, których dane dotyczą ani organu nadzorczego. Przetwarzający zobowiązany jest przekazać, co najmniej następujące informacje:
   a) datę i godzinę zdarzenia (jeśli jest znana; w razie potrzeby możliwe jest określenie w przybliżeniu),
   b) datę i godzinę kiedy Przetwarzający powziął informację o zdarzeniu;

c) opis charakteru i okoliczności naruszenia (w tym wskazanie, na czym polegało naruszenie, określenie miejsca, w którym fizycznie doszło do naruszenia, wskazanie nośników, na których znajdowały się dane będące przedmiotem naruszenia),
d) kategorie i przybliżoną liczbę wpisów (rekordów), których dotyczyło naruszenie,
e) kategorie i przybliżoną liczbę osób, których dotyczyło naruszenie,
f) opis potencjalnych konsekwencji i niekorzystnych skutków naruszenia dla osób, których dane dotyczą,
g) opis środków technicznych i organizacyjnych, które zostały lub mają być zastosowane w celu złagodzenia potencjalnych niekorzystnych skutków naruszenia,
h) imię, nazwisko i dane kontaktowe do osoby, od której można uzyskać więcej informacji na temat zgłoszonego naruszenia.

§ 5. Prawo kontroli

1. Administrator ma prawo w okresie obowiązywania Umowy do przeprowadzenia audytów, w tym inspekcji niezbędnych do wykazania spełnienia obowiązków Przetwarzającego określonych w powszechnie obowiązujących przepisach lub w celu weryfikacji, czy przetwarzanie przez Przetwarzającego powierzonych danych osobowych jest zgodnie z postanowieniami Umowy.
2. O chęci skorzystania z uprawnień, o których mowa w ust. 1 Administrator zobowiązany jest powiadomić Przetwarzającego, na co najmniej 5 dni roboczych (rozumianych jako dni od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy – dalej: „Dni Robocze" chyba że Przetwarzający prowadzi działalność także w dni ustawowo wolny od pracy) przed planowanym audytem, w tym inspekcją.
3. Strony postanawiają, iż realizacja uprawnień, o których mowa w ust. 1 nie będzie mogła utrudniać bieżącej działalności Przetwarzającego.
4. Podczas realizacja uprawnień, o których mowa w ust. 1 Administrator zobowiązany będzie do poszanowania i stosowania się do polityki i regulaminów obowiązujących u Przetwarzającego w zakresie przetwarzania danych osobowych oraz do zachowania w tajemnicy przez okres wskazany przez Przetwarzającego wszelkich informacji stanowiących tajemnicę przedsiębiorstwa Przetwarzającego oraz innych informacji poufnych go dotyczących, w których posiadanie wejdzie Administrator w związku z przeprowadzoną kontrolą.
5. Przetwarzający zobowiązany jest również do umożliwienia przeprowadzenia przez właściwy organ administracji kontroli zgodności przetwarzania danych osobowych (powierzonych Przetwarzającemu do przetwarzania zgodnie z Umową) z powszechnie obowiązującymi przepisami.

§ 6. Dalsze powierzenie przetwarzania danych osobowych

1. Przetwarzający oświadcza, że podwykonawcą któremu zostaną podpowierzone dane osobowe powierzone w Umowie będzie: ……..(należy wskazać podwykonawców)*
2. Strony postanawiają, iż Przetwarzający jest uprawniony do dalszego powierzenia przetwarzania danych osobowych, powierzonych na mocy niniejszej Umowy również innym niż wymieniony w ust. 1 podwykonawcom lub innym podmiotom świadczącym usługi lub prace związane z realizacją Umowy Głównej, przy czym warunkiem skorzystania z tego uprawnienia jest:
   1) uprzednie poinformowanie Administratora o zamiarze dalszego powierzenia przetwarzania danych osobowych danemu podwykonawcy lub innemu podmiotowi świadczącym usługi/prace związane z realizacją Umowy Głównej (potencjalnemu dalszemu przetwarzającemu) lub dokonaniu zmiany w zakresie podmiotu będącego już dalszym przetwarzającym,
   2) brak zgłoszenia przez Administratora sprzeciwu dla zamierzonego dalszego powierzenia przetwarzania danych osobowych w terminie 7 Dni Roboczych licząc od dnia doręczenia mu informacji, o której mowa w pkt a powyżej.

3. Podwykonawca, o którym mowa w §5 ust. 1 i 2 Umowy winien spełniać te same gwarancje i obowiązki, jakie zostały nałożone na Przetwarzającego w Umowie.
4. Przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązkach ochrony danych.

Lub

1. Przetwarzający nie korzysta z usług innego podmiotu przetwarzającego (zwanego dalej Podwykonawcą) bez uprzedniej szczegółowej lub ogólnej pisemnej zgody Administratora. W przypadku ogólnej pisemnej zgody Podmiot przetwarzający informuje Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia Podwykonawców, dając tym samym Administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.
2. Podmiot przetwarzający zapewnia, że na Podwykonawcę nałożone zostaną – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii Europejskiej lub prawu krajowemu – te same obowiązki ochrony danych, jakie na Podmiot przetwarzający nakłada niniejsza umowa, a w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom rozporządzenia.
3. Jeżeli Podwykonawca nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków Podwykonawcy spoczywa na Podmiocie przetwarzającym.

§ 7. Odpowiedzialność Przetwarzającego

1. Przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Przetwarzającego danych osobowych powierzonych na podstawie Umowy, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez powołany administracyjny organ nadzoru przetwarzania danych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora.
2. W zakresie, w jakim jest to dopuszczalne w świetle bezwzględnie obowiązujących przepisów prawnych - całkowita i łączna odpowiedzialność odszkodowawcza Przetwarzającego wobec Administratora z tytułu niewykonania lub nienależytego wykonania niniejszej Umowy, w tym z tytułu niezgodnego z Umową przetwarzania danych osobowych ograniczona jest wyłącznie do udokumentowanej szkody rzeczywistej Administratora (tj. z wyłączeniem w całości utraconych korzyści Administratora). Ograniczenia, o których mowa w zdaniu poprzednim nie odnoszą się do ewentualnych roszczeń regresowych Administratora względem Przetwarzającego w sytuacji, gdy Przetwarzający okaże się odpowiedzialny/współodpowiedzialny za szkodę, którą poniosła osoba, której dane dotyczą w wyniku naruszenia Rozporządzenia, ale wyłącznie w zakresie w jakim Przetwarzający odpowiada zgodnie z ogólnym rozporządzeniem o ochronie danych jako podmiot przetwarzający dane osobowe Administratora na podstawie niniejszej Umowy. Administrator zobowiązany jest każdorazowo do poinformowania Przetwarzającego o każdym zdarzeniu, które mogłoby stanowić podstawę zgłoszenia przez Administratora roszczeń regresowych, o których mowa w zdaniu poprzednim w przypadku, gdy okoliczności zdarzenia wskazują na odpowiedzialność/współodpowiedzialność Przetwarzającego w powstaniu szkody oraz umożliwi Przetwarzającemu odniesienie się i wskazanie okoliczności, które wyłączają obowiązek naprawienia ewentualnej szkody przez Przetwarzającego jako podmiot przetwarzający.

§ 8. Okres obowiązywania umowy

1. Umowa zostaje zawarta na czas określony: od dnia podpisania Umowy Głównej r. do dnia …… r. (tj. okres równy okresowi obowiązywania Umowy Głównej), z zastrzeżeniem ust. 2 i §9 ust. 2.
2. W przypadku podjęcia przez Administratora decyzji o zwrocie danych osobowych lub ich kopii, o których mowa w §4 ust. 6 Umowy termin obowiązywania niniejszej Umowy zostaje wydłużony do dnia upływu terminu wskazanego w §4 ust. 6.
3. Przetwarzanie danych osobowych powierzonych do przetwarzania Przetwarzającemu zgodnie z Umową odbywać się będzie w okresie obowiązywania Umowy.

§ 9. Rozwiązanie Umowy

1. Administrator może rozwiązać Umowę ze skutkiem natychmiastowym, gdy Przetwarzający:
   1) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie nie krótszym niż 14 dni;
   2) przetwarza dane osobowe w sposób niezgodny z Umową;
   3) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora.
2. Umowa ulega również rozwiązaniu bez konieczności składania przez Strony dodatkowych oświadczeń w przypadku rozwiązania lub wypowiedzenia Umowy Głównej.

§ 10. Postanowienia końcowe

1. W przypadku wyznaczenia u Administratora lub odpowiednio u Przetwarzającego osoby pełniącej funkcję inspektora ochrony danych, każda ze Stron powiadomi drugą stronę w formie pisemnej lub elektronicznej o osobie pełniącej u danej Strony funkcję inspektora ochrony danych oraz przekaże dane kontaktowe do tej osoby. W analogiczny sposób Strony będą powiadamiać się wzajemnie o zmianie osoby pełniącej u danej Strony funkcję inspektora ochrony danych.
2. Mając na uwadze, iż niniejsza Umowa zawarta została w związku i w celu realizacji Umowy Głównej Przetwarzający potwierdza, iż kalkulacja wynagrodzenia należnego Przetwarzającemu na podstawie Umowy Głównej została dokonana przy uwzględnieniu zobowiązań Przetwarzającego wynikających z Umowy i zobowiązania określone w niniejszej Umowy zostaną wykonane przez Przetwarzającego w ramach wynagrodzenia określonego w Umowie Głównej.
3. Strony będą dążyć do polubownego rozstrzygnięcia wszelkich sporów, jakie mogą wyniknąć w związku z interpretacją lub wykonywaniem Umowy.
4. Jeżeli działanie podjęte w myśl ust. 3 niniejszego paragrafu nie przyniosą rezultatu zadowalającego obie Strony, sądem właściwym do rozstrzygania wszelkich sporów wynikających z niniejszej Umowy jest sąd powszechny dla siedziby Administratora.
5. Wszelkie zmiany niniejszej Umowy wymagają formy pisemnej pod rygorem nieważności.
6. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Administrator	Przetwarzający
……...……	…….
Podpis osoby lub osób upoważnionej(-ych) do reprezentacji	Podpis osoby lub osób upoważnionej(-ych) do reprezentacji

ZAŁĄCZNIK NR 5. PROTOKÓŁ NADAWANIA I MODYFIKACJI UPRAWNIEŃ PRACOWNIKÓW W SYSTEMACH INFORMATYCZNYCH (WZÓR)

Kopcie, dnia.....

NADANIE POZIOMU UPRAWNIEŃ DO PRACY W SYSTEMACH INFORMATYCZNYCH SŁUŻACYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie obowiązującego w Publicznej Szkole Podstawowej w Kopciach dokumentu „Polityka bezpieczeństwa przetwarzania danych osobowych" zatwierdzam dla:

Pani / Pana ……..……..……
(imię i nazwisko osoby upoważnionej)

zatrudnionej (ego) w ……
(nazwa komórki organizacyjnej)

na stanowisku: ……..……

następujący zakres i poziom uprawnień do pracy w systemach informatycznych :

1. …… w zakresie ……..……..…… *)
nazwa systemu
2. …… w zakresie ……..……..…… *)
nazwa systemu
3. …… w zakresie ……..…..…… *)
nazwa systemu

Osoba uprawniona otrzymuje login …….. do wyżej wymienionych systemów informatycznych.

……..
Podpis Dyrektora

*) wskazać zakres czynności

ZAŁĄCZNIK NR 6. WYKAZ OSÓB UPRAWNIONYCH DO OTWIERANIA I ZAMYKANIA BUDYNKU PUBLICZNEJ SZKOŁY PODSTAWOWEJ W KOPCIACH

Osobami uprawnionymi do posiadania kluczy do drzwi wejściowych, otwierania i zamykania budynku Publicznej Szkoły Podstawowej w Kopciach są niżej wymienione osoby:

imię i nazwisko	stanowisko
Dorota Czajkowska	dyrektor
Honorata Pawlak	woźna

ZAŁĄCZNIK NR 7. KLAUZULA INFORMACYJNA DLA PRACOWNIKÓW

W związku z zawartą umową o pracę/zlecenie/dzieło* zgodnie z art. 13 ust. 1 i ust. 2 ogólnego Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych - RODO) (Dz.U. UE. z 2016 r., L 119, poz. 1) informuję, że:

1. Administratorem Pani/Pana* danych osobowych jest Publiczna Szkoła Podstawowa w Kopciach, Kopcie 21, 07-110 Grębków, tel. 25 793 50 27 .
2. Inspektorem Ochrony Danych jest Pan Marek Daniel, wszelkie pytania związane z przetwarzaniem Pani/Pana* danych osobowych można kierować na adres poczty elektronicznej iod-md@tbdsiedlce.pl.
3. Pani/Pana* dane osobowe przetwarzane będą w celu realizacji obowiązków prawnych pracodawcy/zleceniodawcy* wynikających z umowy o pracę/zlecenie/dzieło* na podstawie przepisów prawa regulujących wskazane formy współpracy oraz przepisów związanych z zabezpieczeniem społecznym.
4. Pani/Pana* dane osobowe będą przechowywane przez okres wskazany przez przepisy prawa regulujące określone formy współpracy.
5. Z wyjątkami określonymi w przepisach prawa posiada Pani/Pan* prawo: dostępu do treści swoich danych, do ich sprostowania, usunięcia, ograniczenia przetwarzania, do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
6. Ma Pan/Pani* prawo wniesienia skargi do właściwego organu nadzorczego w zakresie ochrony danych osobowych gdy uzna Pani/Pan*, iż przetwarzanie danych osobowych Pani/Pana* dotyczących narusza przepisy ogólnego Rozporządzenia o ochronie danych osobowych;
7. Podanie przez Pana/Panią *danych osobowych jest wymagane przepisami prawa właściwego do wskazanej formy współpracy. Jest Pani/Pan* zobowiązana/y do ich podania, a konsekwencją niepodania danych osobowych będzie niemożność zawarcia umowy o prace/zlecenie/dzieło* oraz zrealizowania obowiązków podatkowych i ubezpieczeniowych.
8. Podanie danych oznaczonych na kwestionariuszu symbolem** jest dobrowolne i ich przetwarzanie odbywa się w oparciu o zgodę.
9. Administrator może przekazać/powierzyć Państwa dane innym podmiotom na podstawie przepisów prawa (np. jednostki gminne, administracja skarbowa, podmioty obsługujące sferę socjalną, BHP, p.poż, IOD) lub umowy powierzenia przetwarzania z podmiotami świadczących usługi na rzecz Administratora.

Zostałam/em zapoznana/ny: ……

(imię i nazwisko)

Data ..... ……

(podpis)

* - niepotrzebne skreślić

** - dane osobowe na kwestionariuszu wyróżnione symbolem dla odróżnienia od danych obligatoryjnych wymaganych przepisami prawa

ZAŁĄCZNIK NR 8. KLAUZULA INFORMACYJNA RODO

W związku z zapisami art. 13 oraz art. 14 ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych - RODO) (Dz.U. UE. z 2016 r., L 119, poz. 1) informuję, że Administratorem Państwa danych osobowych jest:

Publiczna Szkoła Podstawowa w Kopciach, Kopcie 21, 07-110 Grębków, tel. 25 793 50 27 .

Informujemy że na mocy art. 37 ust. 1 lit. a) RODO Administrator powołał Inspektora Ochrony Danych (IOD), który w jego imieniu nadzoruje sferę przetwarzania danych osobowych. Z IOD można kontaktować się pod adresem mail: iod-md@tbdsiedlce.pl.

Do zakresu działania Administratora należy wykonywanie zadań publicznych oraz komercyjnych o charakterze kulturalnym, sportowym i rozrywkowym. Administrator gromadzi Państwa dane w celu realizacji zadań wynikających z przepisów prawa oraz pozostałych zadań na podstawie Państwa zgody.

Podstawa prawna przetwarzania Państwa danych wynika z ustawy Prawo Oświatowe i zadań zleconych przez instytucje nadrzędne wobec Administratora oraz na podstawie zgód wyrażonych przez osobę, której dane są przetwarzane. Administrator przetwarza Państwa dane osobowe w ściśle określonym, minimalnym zakresie, niezbędnym do osiągnięcia celu, o którym mowa powyżej.

W zależności od czynności przetwarzania, której poddawane są Państwa dane osobowe w Publicznej Szkole Podstawowej w Kopciach, podanie danych osobowych może być wymagane przepisami prawa, niezbędne do realizacji obowiązku szkolnego lub dobrowolne.

W szczególnych sytuacjach Administrator może przekazać/powierzyć Państwa dane innym podmiotom. Podstawą przekazania/powierzenia danych są przepisy prawa (np. inne jednostki gminne, wymiar sprawiedliwości) lub właściwie skonstruowane, zapewniające bezpieczeństwo danych umowy powierzenia (np. z podmiotami sektora teleinformatycznego i telekomunikacyjnego) zawarte z podmiotami świadczącymi usługi na rzecz Administratora.

Dane osobowe przetwarzane przez Publiczną Szkołę Podstawową w Kopciach przechowywane będą przez okres niezbędny do realizacji celu, dla jakiego zostały zebrane oraz zgodnie z terminami archiwizacji określonymi przez ustawy kompetencyjne lub do czasu odwołania zgody.

Każda osoba, z wyjątkami zastrzeżonymi przepisami prawa, ma możliwość:

- dostępu do danych osobowych jej dotyczących,
- żądania ich sprostowania,
- usunięcia lub ograniczenia przetwarzania,
- wniesienia sprzeciwu wobec przetwarzania.

Z powyższych uprawnień można skorzystać w siedzibie Administratora, pisząc na adres Administratora lub drogą elektroniczną, kierując korespondencję na adres iod-md@tbdsiedlce.pl.

Osoba, której dane przetwarzane są na podstawie zgody wyrażonej przez tę osobę, ma prawo do cofnięcia tej zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.

Przysługuje Państwu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Państwa danych osobowych przez Publiczną Szkołę Podstawową w Kopciach, Kopcie 21, 07-110 Grębków. Organem właściwym dla ww. skargi jest:

Prezes Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

.....

(podpis Administratora)

ZAŁĄCZNIK NR 9. POLITYKA PORZĄDKOWA PRZETWARZANIA

Zobowiązuje wszystkich pracowników i podmioty współpracujące z Administratorem Danych, którym jest:

Publiczna Szkoła Podstawowa w Kopciach, Kopcie 21, 07-110 Grębków, tel. 25 793 50 27 ,

do stosowania się do poniższych zasad.

Nadzór nad ich realizacją sprawuje Inspektor Ochrony Danych.

1. Zasada zamkniętego pomieszczenia – niedopuszczalne jest pozostawienie niezabezpieczonego pomieszczenia służbowego, zarówno w godzinach pracy, jak i po jej zakończeniu, jeżeli nie pozostaje w nim osoba uprawniona. Zasada nie dotyczy pomieszczeń ogólnie dostępnych. Po zakończeniu dnia pracy, ostatnia wychodząca z pomieszczenia osoba jest zobowiązana zamknąć wszystkie okna i drzwi oraz zgodnie z obowiązującymi wewnętrznymi przepisami, zabezpieczyć klucze do pomieszczenia.
2. Zasada nadzorowanych dokumentów – po godzinach pracy wszystkie dokumenty, które zostały uznane za informacje chronione, powinny być przechowywane w zamkniętych szafach lub szufladach, zabezpieczonych przed dostępem do osób nieuprawnionych.
3. Zasada „czystego" biurka – należy unikać pozostawiania bez nadzoru dokumentów na biurku, a w szczególności dokumentów zawierających dane chronione. Po zakończeniu pracy należy uprzątnąć biurko z dokumentów papierowych, płyt CD, DVD lub innych nośników danych.
4. Zasada „czystej" tablicy – po zakończeniu zajęć, spotkań, szkoleń itp. należy uprzątnąć wszystkie materiały oraz pozostawić czystą tablicę (flipchart).
5. Zasada bezpiecznego ekranu – każdy komputer (z wyłączeniem systemów pracy ciągłej) musi mieć ustawiony wygaszacz ekranu z włączoną opcją konieczności zalogowania przy powrocie do pracy, włączający się automatycznie po 5 minutach bezczynności użytkownika. Przed pozostawieniem włączonego komputera bez opieki użytkownicy powinni zablokować go (WIN+L - włączając wygaszacz ekranu) lub w przypadku dłuższej nieobecności wylogować się z systemu. Po zakończonym dniu pracy komputer powinien zostać wyłączony.
6. Zasada odbioru dokumentów z drukarek – dokumenty powinny być zabierane z drukarek natychmiast po wydrukowaniu. W przypadku nieudanej próby drukowania, użytkownik powinien skontaktować się z osobą odpowiedzialną za eksploatację urządzenia, jeżeli zachodzi podejrzenie, iż wydruk zostanie odebrany przez inną osobę.
7. Zasada pustego kosza – dokumenty papierowe, z wyjątkiem materiałów promocyjnych, marketingowych i informacyjnych, powinny być niszczone w sposób uniemożliwiający ich odczytanie w niszczarce lub za pośrednictwem podmiotu zewnętrznego.

ZAŁĄCZNIK NR 10. MINIMALNE WYMAGANIA BEZPIECZEŃSTWA DLA PODMIOTÓW PRZETWARZAJĄCYCH DANE OSOBOWE NA POTRZEBY PUBLICZNEJ SZKOŁY PODSTAWOWEJ W KOPCIACH ORAZ UTRZYMUJĄCYCH JEJ SYSTEMY IT .

Minimalne wymagania bezpieczeństwa wobec systemów teleinformatycznych używanych przez podmioty przetwarzające dane osobowe, których Administratorem jest Publiczna Szkoła Podstawowa w Kopciach.

1. Okresowe weryfikowanie nieautoryzowanych prób użycia zasobów (np. prób złamania zabezpieczeń, uruchamianych w systemie usług i programów) na podstawie logów systemu i programu antywirusowego.
2. Prowadzenie bieżącej aktualizacji i wsparcia producenta dla urządzeń, systemów, aplikacji przetwarzających dane osobowe oraz zapewniających ochronę tych danych.
3. Blokowanie kont wbudowanych nieużywanych kont technicznych oraz zmiana nazw kont wbudowanych typu administrator, gość itp.
4. Stosowanie w systemach kont użytkowników zapewniających rozliczalność.
5. Przeprowadzenie regularnych (przynajmniej raz w roku dla minimum 30% użytkowników) przeglądów uprawnień wykorzystywanych w systemach teleinformatycznych.
6. Wymuszenie zmiany hasła dla użytkowników z prawami administratora co 90 dni lub stosowanie rozwiązań bardziej zaawansowanych np. kart kryptograficznych.
7. Wymuszenie jakości haseł użytkowników z prawami Administratora - 3 z 4 grup znaków, długość minimum 12 znaków lub stosowanie rozwiązań bardziej zaawansowanych np. kart kryptograficznych.
8. Wymuszenie zmiany haseł dla kont systemowych co 12 miesięcy lub stosowanie rozwiązań bardziej zaawansowanych np. kart kryptograficznych..
9. Wymuszenie jakości haseł wykorzystywanych przez aplikacje – min 8 znaków, złożoność 3 z 4 grup znaków lub haseł o długości min 11 różnych znaków lub stosowanie rozwiązań bardziej zaawansowanych np. kart kryptograficznych.
10. Prowadzenie ewidencji zdarzeń i czynności administracyjnych.
11. Zapewnienie przechowywania kopii zapasowych danych w innej lokalizacji niż dane produkcyjne.
12. Zapewnienie ochrony antywirusowej, w takim stopniu w jakim jest to technicznie możliwe.
13. Przechowywanie logów systemów serwerowych przez okres co najmniej 24 miesięcy przy założeniu że co najmniej 1 miesiąc logów dostępny jest on-line.
14. Zapewnienie mechanizmów integralności i poufności przechowywanych logów systemowych.

Wymagania w odniesieniu do użytkowników systemów teleinformatycznych używanych przez podmiot przetwarzający dane osobowe, których Administratorem jest Publiczna Szkoła Podstawowa w Kopciach.

1. Przekazywanie hasła początkowego lub przy resecie użytkownika na zautoryzowany numer telefonu lub osobiście.
2. Stosowanie imiennych kont użytkowników, lub z identyfikatorem z jednoznacznym przypisaniem osoby za nie odpowiedzialnej.

Wymagania bezpieczeństwa w odniesieniu do folderów sieciowych używanych przez podmiot przetwarzający dane osobowe, których Administratorem jest Publiczna Szkoła Podstawowa w Kopciach.

1. Nadawanie uprawnień do dysków sieciowych za pomocą grup użytkowników w przypadku braku możliwości poprzez dostęp poszczególnych kont użytkowników

2. Nadawanie uprawnień odbywa się wyłącznie na udokumentowany wniosek

Wymagania bezpieczeństwa wobec połączenia VPN używanego przez podmiot przetwarzający dane osobowe, których Administratorem jest Publiczna Szkoła Podstawowa w Kopciach.

1. Wymagane jest stosowanie silnego uwierzytelnienia przy dostępie do systemów z sieci publicznej zalecane jest używanie kluczy kryptograficznych, dopuszcza się stosowanie uwierzytelnienia w oparciu o hasło o długości min 32 znaków złożonego z min 2 grup znaków.
2. Wymagane jest logowanie aktywności użytkowników w systemie umożliwiającym dostęp z zewnątrz.
3. Wymagane jest stałe monitorowanie nieudanych prób logowania do systemu.
4. Wymagane jest monitorowanie logowania na to samo konto z dwóch różnych adresów IP.

Wymagania bezpieczeństwa w zakresie stacji roboczych używanych przez podmiot przetwarzający dane osobowe, których Administratorem jest Publiczna Szkoła Podstawowa w Kopciach.

1. Wymagane jest zablokowanie dostępu do BIOS dla nieautoryzowanego użytkownika.
2. Wymagane jest wyłączenie możliwości bootowania systemu z innych nośników niż dysk twardy komputera.
3. Wymagane jest zapewnienie aktualizacji i wsparcia producenta dla systemu operacyjnego i używanych aplikacji.
4. Zapewnienie automatycznego wylogowania/lub uruchomienie wygaszacza z hasłem, użytkownika z systemu po 5 minutach bezczynności.
5. Zaleca się zastąpienie standardowego konta Administratora lokalnego kontem dedykowanym.
6. Wymagane jest zablokowanie konta "gość".
7. Wymagane jest zapewnienie ochrony antywirusowej/antymalware poprzez skaner lokalny lub sieciowy.

Minimalne wymagania bezpieczeństwa organizacyjnego wobec podmiotów przetwarzających dane osobowe, których Administratorem jest Publiczna Szkoła Podstawowa w Kopciach.

1. Opracowanie niezbędnej dokumentacji w obszarze ochrony danych osobowych zgodnie z mającymi zastosowanie regulacjami prawnymi.
2. Wyznaczenie ról i odpowiedzialności w obszarze ochrony danych osobowych.
3. Zapewnienie funkcjonowania procesu obsługi naruszeń bezpieczeństwa danych osobowych.
4. Zapewnienie właściwej świadomości personelu przetwarzającego dane osobowe.
5. Zapewnienie Administratorowi Danych warunków oraz możliwości kontroli przetwarzania danych.

ZAŁĄCZNIK NR 11. REJESTR I PROTOKÓŁ NARUSZEŃ OCHRONY DANYCH OSOBOWYCH (WZÓR)

REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

Administrator Danych	**Publiczna Szkoła Podstawowa w Kopciach**
	07-110 Grębków, Kopcie 21
	tel. 25 793 50 27
Inspektor Ochrony Danych	Marek Daniel
	iod-md@tbdsiedlce.pl

Nr	Data	Opis
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		

PROTOKÓŁ NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Data		**Nr**	……..
Obowiązek zgłoszenia do PUODO	Tak / Nie		
Obowiązek zawiadomienia osoby której dane dotyczą	Tak / Nie		
Źródło informacji o naruszeniu			
Rodzaj naruszenia			
Okoliczności naruszenia			
Skutki naruszenia			
Podjęte działania zaradcze			

ZAŁĄCZNIK NR 12. PROCEDURA ODTWARZANIA SYSTEMU PO AWARII, ORAZ ICH TESTOWANIA

Procedura odtwarzania systemu po awarii, oraz ich testowania

Procedura odtwarzania systemu po awarii opiera się na następujących założeniach:

- na serwerach jest uruchomiona i skonfigurowana „kopia zapasowa systemu Windows serwer",
- na stacjach roboczych jest uruchomione i skonfigurowane „przywracanie systemu"
- wszystkie krytyczne zasoby danych (bazy danych, konfiguracje baz danych, pliki użytkowników, konfiguracje programów dziedzinowych) są regularnie archiwizowane w okresach adekwatnych do zmian zawartości chronionych zasobów (po każdej zmianie konfiguracji sprzętu sieciowego (routery, przełączniki itp.), zawartości bazy danych, zmian w systemie operacyjnym,
- archiwizacja jest replikowana w innej lokalizacji niż podstawowe pliki archiwizacji,
- konfiguracja sprzętu, użytkownicy systemów operacyjnych , konfiguracja baz danych, programów dziedzinowych oraz położenie plików użytkowników oraz konfiguracja urządzeń jest opisana w odpowiedniej dokumentacji,
- hasła administracyjne do systemów i urządzeń są zdeponowane w bezpiecznej lokalizacji.

1. Awaria sprzętu komputerowego

1.1. Awaria programu

1. Jeżeli program komputerowy nie działa prawidłowo należy sprawdzić konfigurację programu oraz uprawnienia na zgodność z zapisami w dokumentacji.
2. Jeżeli konfiguracja jest prawidłowa należy przywrócić system do poprzedniego punktu przywracania (w szczególności zwrócić uwagę na punkty przywracania związane z aktualizacjami Windows, odtworzyć program z kopii zapasowej lub zainstalować program na nowo przywracając pierwotną konfigurację.

1.2. Awaria systemu operacyjnego lub komputera (stacji roboczej)

1) Jeżeli system uruchamia się ale nie pracuje prawidłowo należy przywrócić go wcześniejszego stanu – jeżeli jest to możliwe należy przeanalizować logi systemu aby określić przyczynę awarii i czas jej wystąpienia.
2) Jeżeli system nie uruchamia się należy uruchomić komputer z nośnika instalacyjnego i wykonać naprawę systemu Windows lub przywrócenie do poprzedniego poprawnego stanu.
3) Jeżeli przyczyną jest wadliwy dysk należy wymienić dysk na sprawny , odtworzyć system z obrazu lub zainstalować i skonfigurować system zgodnie z dokumentacją konfiguracji (konta użytkownicy)
4) W przypadku awarii np. płyty głównej należy podjąć próbę uruchomienia systemu ze starego dysku
5) W przypadku wymiany całej jednostki działanie jak w pkt. 3)

1.3. Awaria serwera

1) Awaria macierzy dyskowej
   W przypadku awarii dysku w macierzy należy wymienić uszkodzony dysk na sprawny zgodnie z procedurą producenta sprzętu
2) Awaria sprzętu

Jeżeli uległ awarii dysk nie będący elementem macierzy, macierz dyskowa lub inne elementy **uniemożliwiające szybkie odtworzenie systemu** należy zainstalować programy i bazy danych na dowolnym komputerze zastępczym o wystarczających parametrach technicznych aby umożliwić jak najszybsze podjęcie pracy przez użytkowników. Po zakończeniu procedury naprawy serwera należy odtworzyć system z kopii zapasowej. Po odtworzeniu pierwotnego środowiska serwera należy przenieść zasoby z komputera zastępczego na serwer.

W przypadku wymiany serwera na nowy należy odtworzyć na nim środowisko zgodne z używanym lub zainstalować nowe środowisko (np. nowy serwer ma znacznie większe możliwości od uszkodzonego, posiada nowe funkcjonalności.

2. Awaria sprzętu sieciowego

1) W przypadku awarii programowej urządzenia należy je zresetować do ustawień domyślnych a następnie przywrócić konfigurację z archiwizacji.
2) W przypadku awarii fizycznej
   a) Przy wymianie na sprzęt zgodny programowo z uszkodzonym – otworzyć konfigurację z archiwizacji
   b) Przy wymianie na sprzęt niezgodny programowo – odtworzyć konfigurację na funkcjonalnie identyczną na podstawie opisu konfiguracji