Szkoła Podstawowa Nr 1
im. Gen. Franciszka Kleeberga
ul. Piłsudskiego 35
05-091 Ząbki

tel./fax.: (22) 781-61-93
e-mail: sekretariat@sp1zabki.pl

SP1.0211.3.2018

Ząbki, dnia 25 maja 2018 r.

Zarządzenie nr 3/2018
Dyrektora Szkoły Podstawowej nr 1 im. gen. F. Kleeberga w Ząbkach
z dnia 25 maja 2018 r.
w sprawie wprowadzenie
Polityki przetwarzania danych osobowych

Na podstawie 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 95/45/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L nr 119 z 04.05.2016 r.) zarządza się, co następuje:

§ 1

W celu zapewnienia bezpieczeństwa danych osobowych gromadzonych i przetwarzanych przez Administratora Danych Osobowych jakim jest Szkoła Podstawowa nr 1 im. gen. Franciszka Kleeberga w Ząbkach zatwierdzam Politykę przetwarzania danych osobowych stanowiącą załącznik nr 1 do zarządzenia.

§ 2

Na stanowisko Inspektora Ochrony Danych Osobowych zostaje powołany dotychczasowy Administrator Danych Osobowych pan Radosław Wasilewski.

§ 3

Traci moc zarządzenie nr 16/2010/2011 z dnia 20 czerwca 2011 r.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR SZKOŁY
mgr Agnieszka Piskorek

Załącznik nr 1
do Zarządzenia nr 3/2018 Dyrektora
Szkoły Podstawowej nr 1
im. Gen. F. Kleeberga w Ząbkach
z dnia 25 maja 2018 r.

POLITYKA PRZETWARZANIA DANYCH OSOBOWYCH

§ 1. Definicje

Użyte w niniejszej Polityce definicje oznaczają:

- Administrator danych – Szkoła Podstawowa Nr 1 im. Generała Franciszka Kleeberga w Ząbkach, z siedzibą przy ul. Piłsudskiego 35, 05-093 Ząbki,
- Inspektor Ochrony Danych – osoba, o której mowa w art. 37-39 RODO,
- Administrator systemu informatycznego – osoba lub podmiot odpowiedzialny za sprawność, konserwację oraz wdrażanie i monitorowanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych,
- system informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
- stacja robocza – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie,
- bezpieczeństwo systemu informatycznego – wdrożenie przez Administratora danych lub osobę przez niego upoważnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed naruszeniem ochrony danych osobowych,
- użytkownik systemu – osoba przetwarzająca dane osobowe na polecenie Administratora danych oraz uprawniona do przetwarzania danych osobowych w systemie informatycznym,
- Rozporządzenie lub RODO – 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 (ogólne rozporządzenie o ochronie danych),
- pracownik – osoba zatrudniona przez Administratora danych na podstawie umowy o pracę lub umowy cywilnoprawnej, której praca lub usługi wiążą się z przetwarzaniem danych osobowych,
- klauzula informacyjna – informacja zapewniająca przejrzystość przetwarzania danych osobowych, szczególnie spełniająca przesłanki wskazane w art. 13 i art. 14 RODO.

§ 2. Deklaracja Administratora danych

1. Administrator danych w celu zapewnienia właściwej i skutecznej ochrony danych osobowych deklaruje:

- zamiar podejmowania wszystkich działań niezbędnych dla ochrony danych osobowych osób fizycznych,
- zamiar stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe w Szkole w zakresie problematyki bezpieczeństwa tych danych,
- zamiar podejmowania w niezbędnym zakresie współpracy z instytucjami powołanymi do ochrony danych osobowych,
- stosowanie i regularne przeglądanie i monitorowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych

odpowiednich do zagrożeń oraz kategorii danych objętych ochroną,
- prowadzenie okresowych sprawdzeń, audytów zgodności działania z aktualnie obowiązującymi wymogami prawnymi.

2. Do obowiązków Administratora danych należy:
- podział zadań i obowiązków związanych z organizacją ochrony danych osobowych,
- podejmowanie niezbędnych i odpowiednich kroków mających na celu zapewnienie prawidłowej ochrony danych osobowych,
- wprowadzenie procedur zapewniających prawidłowe przetwarzanie danych osobowych,
- egzekwowanie rozwoju środków bezpieczeństwa przetwarzania danych osobowych,
- zapewnienie niezbędnych środków potrzebnych dla zapewnienia bezpieczeństwa przetwarzanych danych osobowych,
- wydawanie poleceń przetwarzania danych osobowych.

3. Administrator danych w porozumieniu z Burmistrzem Ząbek powołuje Inspektora Ochrony Danych, którego zadania określa § 5.

4. Administrator danych powołuje Administratora systemów informatycznych, którego zadania określa § 6.

§ 3. Zakres i cele Polityki

1. Politykę stosuje się do danych osobowych przetwarzanych przez Administratora danych metodą tradycyjną, w systemach informacyjnych, zapisanych na zewnętrznych nośnikach informacji oraz informacji dotyczących bezpieczeństwa przetwarzania danych osobowych, w szczególności dotyczących wdrożonych zabezpieczeń technicznych i organizacyjnych.

2. Polityka jest zestawem praw, reguł i praktycznych wskazówek ochrony i przetwarzania danych osobowych w Szkole. Określa sposób prowadzenia dokumentacji związanej z przetwarzanymi danymi osobowymi, ponadto określa środki techniczne i organizacyjne zastosowane do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych. Jest zbiorem reguł określającym dopuszczalne granice zachowania się wszystkich pracowników przetwarzających dane osobowe.

3. Celem Polityki jest określenie kierunków działań oraz wsparcia dla zapewnienia bezpieczeństwa przetwarzania danych osobowych w celu prawidłowej ochrony przetwarzanych danych osobowych.

4. W zakresie podmiotowym, Polityka obowiązuje wszystkich pracowników Administratora danych, inne osoby mające dostęp do danych osobowych (m. in. stażystów, praktykantów, wolontariuszy, osoby zatrudnione na umowę zlecenie lub umowę o dzieło), a także podmioty, którym na mocy umowy lub innego instrumentu prawnego Administrator wydał polecenie przetwarzania danych osobowych.

§ 4. Zarządzanie ochroną danych osobowych

1. Administrator danych zabezpiecza dane osobowe przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieupoważnioną, przetwarzaniem z naruszeniem przepisów RODO, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Bez względu na zajmowane stanowisko, miejsce wykonywania pracy oraz charakter stosunku pracy lub rodzaj umowy cywilnoprawnej, zasady określone w niniejszej Polityce oraz w dokumentach powiązanych powinny być znane i stosowane przez pracowników oraz w niezbędnym zakresie przez współpracowników Administratora danych.

3. Środki techniczne i organizacyjne stosowane do ochrony danych osobowych stosowane przez Administratora danych zawarte są w Rejestrze czynności przetwarzania i są na bieżąco uaktualniane.

4. Dopuszcza się wydawanie poleceń i innych procedur regulujących szczegółowo dany proces przetwarzania danych.

§ 5. Inspektor Ochrony Danych

1. Wszystkie sprawy związane z przetwarzaniem danych osobowych są opiniowane przez IOD.

2. Zakres zadań IOD w szczególności określa art. 39 RODO.

3. Podaje się do publicznej wiadomości dane kontaktowe IOD w postaci numeru telefonu oraz adresu email.

4. W razie nieobecności w pracy IOD jest zastępowany przez osobę wskazaną przez Administratora danych.

5. IOD opracowuje na każdy rok plan audytów i sprawdzeń, które mają zapewnić przetwarzanie danych w sposób zgodny z prawem.

6. Do zadań IOD należy kontaktowanie się z organem nadzorczym we wszystkich sprawach dotyczących ochrony danych osobowych, przewidzianych przepisami prawa.

7. IOD dokonuje analizy spraw, które powinny być konsultowane z organem nadzorczym.

8. IOD prowadzi ewidencję naruszeń i incydentów.

§ 6. Administrator systemu informatycznego

Do obowiązków Administratora systemów informatycznych ("ASI") należy przede wszystkim:

- zabezpieczenie systemu informatycznego, w którym przetwarzane są dane osobowe przed ingerencją osób trzecich,
- bieżący nadzór oraz zapewnienie ciągłości działania systemu informatycznego,
- reagowanie w przypadku naruszenia, podejrzenia naruszenia bądź powstania zagrożenia bezpieczeństwa danych osobowych,
- nadzór nad naprawami, konserwacją, likwidacją urządzeń służących do przetwarzania danych osobowych,
- przyznawanie określonych praw dostępu do danych osobowych przetwarzanych w systemie informatycznym,
- świadczenie pomocy technicznej użytkownikom systemu informatycznego,
- wykonywanie i zarządzanie kopiami zapasowymi oprogramowania systemu informatycznego,
- wykonywanie oraz przechowywanie dokumentacji należącej do kompetencji ASI,

- monitorowanie osiągnięć technicznych w dziedzinie bezpieczeństwa systemów informatycznych i zgłaszanie ich Administratorowi danych,
- tworzenie projektów umów dotyczących powierzenia przetwarzania danych osobowych, jeżeli przetwarzanie będzie następowało w systemie informatycznym,
- analizowanie możliwości i wprowadzanie mechanizmów szyfrowania danych osobowych w systemach teleinformatycznych,
- inne czynności zlecone przez Administratora danych.

§ 7. Pracownicy

1. Do obowiązków Pracowników należy:
   - dbanie, aby przetwarzanie odbywało się zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,
   - przetwarzanie danych w sposób dokładny, adekwatny, istotny i nie nadmierny w stosunku do celu przetwarzania,
   - usuwanie danych zbędnych, nieprzydatnych i tych, dla których ustał już cel przetwarzania,
   - stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych, odpowiednich do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem,
   - określanie celów, w jakich mają być przetwarzane dane osobowe, zakresu oraz, o ile jest to możliwe, czasu trwania przetwarzania danych osobowych,
   - określanie sposobu przetwarzania danych osobowych,
   - zapewnianie aktualności oraz merytorycznej poprawności danych osobowych,
   - realizacja obowiązku informowania o przetwarzaniu danych osobowych osób, których dane są przetwarzane,
   - udostępnienie danych osobowych odbiorcom,
   - reagowanie i realizacja prawa cofnięcia zgody na przetwarzanie danych osobowych,
   - wypełnianie, na żądanie uprawnionych osób, obowiązków określonych w art. 15-22 RODO,
   - zgłaszanie IOD każdego nowego procesu przetwarzania danych osobowych, podając podstawę prawną przetwarzania, cel, zakres i sposób zbierania danych osobowych,
   - zgłaszanie IOD aktualizacji danych dotyczących zdefiniowanych procesów przetwarzania,
   - przestrzeganie zakresu wydanego polecenia przetwarzania danych osobowych,
   - zachowanie w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia przez cały okres zatrudnienia lub współpracy a także po jego ustaniu,
   - przestrzeganie obowiązków związanych z otwieraniem i zamykaniem pomieszczeń, a także wejścia do obszarów przetwarzania danych osobowych osób nieupoważnionych,
   - przygotowywanie projektu umowy powierzenia przetwarzania danych osobowych podmiotom zewnętrznym lub polecenia przetwarzania danych osobowych,
   - informowanie o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz podatnościach systemu teleinformatycznego przetwarzającego dane osobowe,
   - wykonywanie innych obowiązków wynikających z niniejszej Polityki lub innych procedur dotyczących danych osobowych.

2. Przetwarzanie zgodnie z prawem oznacza ustalanie i weryfikację na każdym etapie przetwarzania czy przetwarzanie odbywa się na co najmniej jednej z przesłanek określonych w art. 6 lub art. 9 RODO.

3. W przypadku stwierdzenia, że przetwarzanie odbywa się bez podstawy prawnej, pracownik zobowiązany jest do zaprzestania dalszego przetwarzania i poinformowania o tym IOD.

4. Przetwarzanie danych osobowych w sposób przejrzysty dla osoby, której dane dotyczą odbywa się w szczególności na podstawie art. 13 i art. 14 RODO.

§ 8. Polecenia przetwarzania danych osobowych

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby, którym Administrator danych wydał polecenie przetwarzania danych.

2. Polecenie powinno być wydane przed rozpoczęciem przetwarzania danych osobowych.

3. Przed rozpoczęciem przetwarzania danych osobowych, osoba, której Administrator danych wydaje polecenie przetwarzania danych musi być przeszkolona z zakresu ochrony danych osobowych, a następnie oświadcza, że została zapoznana, rozumie i będzie przestrzegać obowiązków wynikających z RODO, innych przepisów oraz innych dokumentów obowiązujących u Administratora danych, dotyczących ochrony danych osobowych i zobowiązuje się do zachowania danych osobowych w tajemnicy, również po ustaniu zatrudnienia lub zakończeniu współpracy oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

4. Wzór polecenia przetwarzania stanowi załącznik nr 1 do Polityki.

5. Administrator danych prowadzi ewidencję poleceń wg wzoru stanowiącego załącznik nr 2 do Polityki.

6. Polecenia przetwarzania przechowywane są w aktach osobowych pracownika (lub innym, zbiorczym miejscu) i obowiązują do czasu ustania stosunku pracy lub wygaśnięcia umowy cywilnoprawnej lub obowiązków związanych z przetwarzaniem danych osobowych albo do cofnięcia polecenia.

7. Administrator danych wydaje polecenie przetwarzania lub cofa je na wniosek bezpośredniego przełożonego osoby, która ma być dopuszczona do przetwarzania danych.

8. Polecenie przetwarzania danych osobowych przygotowuje komórka organizacyjna do spraw kadr, na wniosek przełożonego pracownika lub Administratora danych.

9. Przełożony pracownika lub Administrator danych jest zobowiązany, niezwłocznie po ustaniu potrzeby przetwarzania danych osobowych przez pracownika, złożyć do referatu do spraw kadr, do IOD oraz do ASI wniosek o cofnięcie polecenia przetwarzania danych osobowych. IOD – odnotowuje ten fakt w ewidencji poleceń. ASI – usuwa skrzynkę e-mailową pracownika oraz blokuje jego dostęp do systemów informatycznych.

§ 9. Polityka szkoleniowa w zakresie danych osobowych

1. Celem polityki szkoleniowej w zakresie ochrony danych osobowych jest stałe podnoszenie kwalifikacji, wiedzy i kompetencji pracowników oraz współpracowników, mające na celu zapewnianie przestrzegania przepisów o ochronie danych osobowych, zapewnienie prawidłowego przetwarzania danych oraz ochronę tych danych.

2. Szkolenie powinno obejmować następujące zagadnienia:
   - przepisy o ochronie danych osobowych,
   - zasady bezpiecznego użytkowania urządzeń i systemów informatycznych służących do przetwarzania danych osobowych,
   - zagrożenia, na jakie może być narażone przetwarzania danych osobowych, a w szczególności te związane z przetwarzaniem danych osobowych w systemach informatycznych,
   - zasady dostępu do pomieszczeń, w których przetwarzane są dane osobowe,
   - prawa osób, których dane osobowe dotyczą,
   - sposób postępowania w przypadku naruszenia ochrony danych osobowych lub systemu informatycznego,
   - odpowiedzialność z tytułu naruszenia ochrony danych osobowych.

3. Wszystkie osoby wytypowane do przetwarzania danych osobowych, przed dopuszczeniem do przetwarzania oraz przed wydaniem polecenie przetwarzania, muszą zostać przeszkolone w zakresie ochrony danych osobowych. Za opracowanie programu szkolenia i przeprowadzenie szkolenia odpowiada IOD.

4. Szkolenie w zakresie danych osobowych przeprowadza się każdorazowo po zaistnieniu zdarzenia zidentyfikowanego, jako incydent naruszenia ochrony danych osobowych, dla całej Szkoły, grupy pracowników lub pracownika – w zależności od rodzaju incydentu.

5. Szkolenia powinny być powtarzane okresowo lub na żądanie, gdy zaistnieje taka potrzeba.

§ 10. Przebywanie w obszarach przetwarzania danych osobowych

1. Administrator danych osobowych wskazuje obszary przetwarzania danych osobowych zgodnie z załącznikiem nr 3 do Polityki.

2. Administrator danych weryfikuje i uaktualnia obszary przetwarzania danych osobowych po każdej istotnej zmianie w tym zakresie.

3. Administrator danych stosuje środki techniczne i organizacyjne ograniczające powszechny dostęp do kluczy do wszystkich pomieszczeń i budynków wchodzących w skład obszaru przetwarzania danych osobowych (np. szafki na klucze zabezpieczone kodem).

4. Osoby, którym Administrator danych wydał polecenie przetwarzania danych osobowych są jednocześnie upoważnione do przebywania w obszarach przetwarzania danych osobowych.

5. Przebywanie w obszarach przetwarzania danych osobowych osób nieuprawnionych jest dopuszczalne tylko w obecności osoby uprawnionej.

6. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane podczas nieobecności osób uprawnionych, w sposób wykluczający dostęp do nich osobom nieuprawnionych.

7. Osoby uprawnione zobowiązane są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszaru przetwarzania w czasie ich chwilowej nieobecności w pomieszczeniu, a klucze nie mogą być pozostawione w zamku drzwi.

8. Zakazuje się wynoszenia kluczy po zakończeniu pracy poza miejsce przeznaczone do ich przechowywania oraz och dorabiania, za wyjątkiem osób upoważnionych do dokonania tego działania.

9. Administrator danych może uprawnić osoby, którym nie wydał polecenia przetwarzania danych osobowych, do dostępu do pomieszczeń, w których przetwarzane są dane osobowe.

§ 11. Przetwarzanie danych osobowych w systemie informatycznym

1. Dane osobowe mogą być przetwarzane w systemie informatycznym wyłącznie przez osoby, którym Administrator danych wydał stosowne polecenie przetwarzania.

2. Dostęp do systemu informatycznego może mieć miejsce wyłącznie po podaniu identyfikatora i aktualnego hasła.

3. ASI generuje i przydziela identyfikator i pierwsze hasło użytkownika do logowania do systemu informatycznego na podstawie wniosku bezpośredniego przełożonego osoby, która ma być dopuszczona do przetwarzania danych w systemie informatycznym.

4. ASI wyrejestrowuje lub zmienia zakres uprawnień dostępu użytkownika z systemu informatycznego na podstawie wniosku bezpośredniego przełożonego osoby, z którą ustał lub wygasł stosunek pracy lub umowa cywilnoprawna, której zmieniono zakres obowiązków lub zakończono współpracę.

5. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Identyfikator składa się minimalnie z pięciu znaków, określających imię i nazwisko pracownika rozdzielone kropką ewentualnie pierwszą literę imienia i nazwisko pracownika rozdzielone kropką.

6. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielany innej osobie.

7. System informatyczny przetwarzający dane osobowe jest skonfigurowany w sposób wymagający bezpieczne zarządzanie hasłami użytkowników:
- hasło przydzielone użytkownikowi musi być zmienione po pierwszym udanym zalogowaniu się do systemu informatycznego,
- zastosowano mechanizm wymuszający zmianę hasła po upływie 30 dni od dnia ostatniej zmiany hasła,
- zastosowano mechanizm pozwalający na wymuszanie jakości hasła, w szczególności hasło powinno składać się z co najmniej 8 znaków, powinno zawierać małe i wielkie litery oraz cyfry i znaki specjalne.

8. Osoby upoważnione do wykonywania prac administracyjnych w systemie informatycznym posiadają własne konto administracyjne, do których mają przydzielone hasło. Zasady zarządzania hasłami są analogiczne, jak w przypadku haseł użytkowników. Nazwa i hasło użytkownika posiadających uprawnienia ASI powinny być przechowywane w zamkniętej szafie, do której dostęp jest w pełni kontrolowany, przy czym dostęp do tych szaf ma wyłącznie

Administrator danych lub osoba przez niego upoważniona. Nazwa użytkownika oraz hasło powinny być przechowywane w opieczętowanej i opatrzonej podpisem ASI kopercie. W przypadku konieczności awaryjnego użycia nazwy i hasła użytkownika konieczny jest wpis odnotowujący zaistniałą sytuację w "Dzienniku haseł" znajdującym się w szafie wraz z kopertą, w której znajdują się hasła. Wpis powinien zawierać następujące informacje:

- imię, nazwisko oraz stanowisko osoby upoważnionej udostępniającej dostęp do szafy, w której znajdują się hasła,
- imię, nazwisko oraz stanowisko osoby, która pobiera nazwy użytkowników i hasła,
- krótki opis sytuacji, która wymusiła awaryjne wykorzystanie haseł.

9. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.

10. W przypadku bezczynności użytkownika na stacji roboczej przez okres dłuższy niż 10 minut automatycznie włączany jest wygaszacz ekranu. Wygaszacze ekranu są zaopatrzone w hasła zbudowane analogicznie do haseł używanych przez użytkownika przy logowaniu.

11. Zmianę użytkownika systemu informatycznego każdorazowo musi poprzedzać wylogowanie się poprzedniego użytkownika. Niedopuszczalne jest, aby dwóch lub większa ilość użytkowników wykorzystywała wspólnie jedno konto użytkownika.

12. W przypadku, gdy przerwa w pracy na stacji roboczej trwa dłużej niż 5 minut użytkownik zobowiązany jest wylogować się z aplikacji i systemu stacji roboczej, na której pracuje oraz sprawdzić, czy nie zostały pozostawione bez zamknięcia elektroniczne nośniki informacji zawierające dane osobowe.

13. W pomieszczeniach, w których przetwarzane są dane i w których jednocześnie mogą przebywać osoby postronne, monitory powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w dane lub powinny być zaopatrzone w filtr prywatyzujący.

14. Zakończenie pracy użytkownika w systemie informatycznym obejmuje zamknięcie aplikacji i zakończenie pracy w sieci.

§ 12. Procedura tworzenia kopii zapasowych

1. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada ASI lub osoba specjalnie do tego celu wyznaczona.

2. Dokumenty elektroniczne zawierające dane osobowe, powstałe w wyniku przetwarzania danych, jeśli nie zachodzi potrzeba ich archiwizacji, są niezwłocznie i trwale usuwane ze stacji roboczej.

3. Kopie zapasowe informacji przechowywanych w systemie informatycznym przetwarzającym dane osobowe tworzone są w następujący sposób:

- kopia zapasowa oprogramowania przetwarzającej dane osobowe – pełna kopia wykonywania jest po wprowadzeniu zmian do oprogramowania, kopie umieszczone są na nośnikach wymiennych, kopia przechowywana jest w zamkniętej szafie pancernej,
- kopia zapasowa danych osobowych przetwarzanych przez oprogramowanie wykonywana jest codziennie na dysku lokalnym komputera wybranego przez ASI (komputerem tym nie może być serwer baz danych),

- raz w tygodniu, na elektronicznym nośniku, tworzona jest kopia zawierająca kopię zapasową danych osobowych z każdego dnia ostatniego tygodnia, kopia ta przechowywana jest w zamkniętej szafie pancernej, w innym pomieszczeniu niż znajdują się serwery danych,
- zbiorcze (tygodniowe) kopie zapasowe przechowywane są przez okres dwóch tygodni, po tym terminie stare kopie są trwale usuwane,
- kopia zapasowa danych konfiguracyjnych systemu informatycznego przetwarzającego dane osobowe, w tym uprawnień użytkowników systemu – pełna kopia wykonywana jest raz na miesiąc, przechowywana jest w zamkniętej szafie pancernej.

4. Do tworzenia kopii zapasowych wykorzystywane sa dedykowane do tego celu urządzenia wchodzące w skład systemu informatycznego na nośnikach wymiennych adekwatnych do rodzaju urządzenia.

5. W przypadku przechowywania kopii zapasowej przez okres dłuższy niż pół roku, wszystkie kopie zapasowe zbiorów danych osobowych, aplikacji przetwarzających dane osobowe, których to dotyczy musza być okresowo (co najmniej raz na pół roku) sprawdzane pod względem ich dalszej przydatności. Czynności te wykonuje ASI.

6. Nośniki kopii zapasowych, które zostały wycofane z użycia, jeżeli jest to możliwe, należy pozbawić zapisanych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych. W przeciwnym wypadku podlegają fizycznemu zniszczeniu z wykorzystaniem metod adekwatnych do typu nośnika, w sposób uniemożliwiający odczytanie zapisanych na nich danych.

§ 13. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

1. Nośniki danych osobowych, zarówno w postaci elektronicznej, jak i papierowej powinny być zabezpieczone przed dostępem osób nieuprawnionych, nieautoryzowaną modyfikacją i zniszczeniem. Dane osobowe mogą być zapisywane na nośnikach przenośnych w przypadku tworzenia kopii zapasowych lub gdy istnieje konieczność przeniesienia tych danych w postaci elektronicznej, a wykorzystanie do tego celu sieci informatycznej jest nieuzasadnione, niemożliwe lub zbyt niebezpieczne.

2. Nośniki danych osobowych oraz wydruki powinny być przechowywane w zamkniętych szafach wewnątrz obszaru przetwarzania danych osobowych i nie powinny być bez uzasadnionej przyczyny wynoszone poza ten obszar.

3. W przypadku, gdy nośnik danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie nośnika lub usunięcie danych z nośnika zgodnie ze wskazówkami zamieszczonymi w rozdziale Procedura tworzenia kopii zapasowych. Jeżeli wydruk danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie wydruku przy użyciu niszczarki dokumentów.

4. W przypadku, gdy kopia zapasowa nie jest dłużej potrzebna, należy przeprowadzić jej zniszczenie lub usunięcie danych z nośnika, na którym się ona znajduje zgodnie z zasadami zamieszczonymi w rozdziale Procedura tworzenia kopii zapasowych.

§ 14. Sposób zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania

1. W związku z tym, że system informatyczny narażony jest na działanie szkodliwego oprogramowania, którego celem może być uzyskanie nieuprawnionego dostępu do tego systemu, konieczne jest podjęcie odpowiednich środków ochronnych.

2. Można wyróżnić następujące rodzaje występujących zagrożeń:
   - nieuprawniony dostęp bezpośrednio do bazy danych,
   - uszkodzenie kodu aplikacji umożliwiającej dostęp do bazy danych w taki sposób, że przetwarzane dane osobowe ulegną zafałszowaniu lub zniszczeniu,
   - przechwycenie danych podczas transmisji w przypadku rozproszonego przetwarzania danych z wykorzystywaniem ogólnodostępnej sieci Internet,
   - przechwycenie danych z aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych przez wyspecjalizowany program szpiegowski i nielegalne przesłanie tych danych poza miejsce przetwarzania danych,
   - uszkodzenie lub zafałszowanie danych osobowych przez wirus komputerowy zakłócający prace aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych.

3. W celu przeciwdziałania wymienionym zagrożeniom system informatyczny musi posiadać następujące zabezpieczenia:
   - fizyczne odseparowanie serwera bazy danych od sieci zewnętrznej,
   - autoryzacja użytkowników przy zachowaniu odpowiedniego poziomu komplikacji haseł dostępu,
   - stosowanie rygorystycznego systemu autoryzacji dostępu do wszystkich serwerów, na których znajdują się elementy aplikacji umożliwiających przetwarzanie danych osobowych,
   - stosowanie aplikacji w postaci skomplikowanej i nie umieszczenie kodu źródłowego aplikacji na powszechnie dostępnych serwerach,
   - stosowanie szyfrowanej transmisji danych przy użyciu odpowiedniej długości klucza szyfrującego,
   - stosowanie odpowiedniej ochrony antywirusowej na stacjach roboczych wykorzystywanych do przetwarzania danych osobowych.

4. Potencjalnymi źródłami przedostania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są:
   - załączniki do poczty elektronicznej,
   - przeglądane strony internetowe,
   - pliki i aplikacje pochodzące z nośników wymiennych uruchamiane i odczytywane na stacji roboczej.

5. W celu zapewnienia ochrony antywirusowej ASI przetwarzającego dane osobowe jest odpowiedzialny za zarządzanie systemem wykrywającym i usuwającym wirusy.

6. System antywirusowy powinien być skonfigurowany w następujący sposób:
   - rezydentny monitor antywirusowy (uruchomiony w pamięci operacyjnej stacji roboczej) powinien być stale włączony,
   - antywirusowy skaner ruchu internetowego powinien być stale włączony,
   - monitor zapewniający ochronę przed wirusami makr w dokumentach MS Office

powinien być stale włączony.

7. Systemy antywirusowe zainstalowane na stacjach roboczych powinny być skonfigurowane w następujący sposób:
- zablokowanie możliwości ingerencji użytkownika w ustawienia oprogramowania antywirusowego,
- możliwość centralnego uaktualnienia wzorców wirusów.

8. System antywirusowy powinien być aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania.

9. Użytkownicy systemu informatycznego zobowiązani są do następujących działań:
- skanowania zawartości dysków stacji roboczej pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów – przynajmniej raz w tygodniu,
- skanowania zawartości nośników wymiennych odczytywanych na stacji roboczej pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów – przy każdym odczycie,
- skanowanie informacji przesyłanych do systemu informatycznego pod kątem pojawienia się niebezpiecznych kodów – na bieżąco.

10. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy ASI powinien podjąć działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:
- usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,
- odtworzenie plików z kopii zapasowych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,
- samodzielna ingerencję w zawartości pliku – w zależności od posiadanych kwalifikacji lub skonsultowanie się z zewnętrznymi ekspertami.

11. System informatyczny przetwarzający dane osobowe powinien posiadać mechanizmy pozwalające na zabezpieczenie ich przed utratą lub wystąpieniem zafałszowania w wyniku awarii zasilania lub zakłóceń w sieci zasilającej. W związku z tym system informatyczny powinien być wyposażony w co najmniej:
- filtry zabezpieczające stacje robocze przed skutkami przepięcia,
- zasilacze awaryjne serwerów baz danych, serwerów aplikacji oraz urządzeń pamięci masowej pozwalające na bezpieczne zamknięcie aplikacji przetwarzających dane osobowe w sposób umożliwiający poprawne zapisanie przetwarzanych danych.

§ 15. Udostępnianie danych

1. Udostępnianie danych osobowych odbywające się na żądanie jest dopuszczone wyłącznie na podstawie obowiązujących przepisów prawa.

2. Wniosek o udostępnienie danych osobowych stanowi załącznik nr 4 do Polityki.

§ 16. Sposób realizacji wymogów odnośnie ewidencji wpisów i udostępnień danych

1. System informatyczny przetwarzający dane osobowe musi posiadać mechanizm uwierzytelniający użytkownika, wykorzystujący identyfikator i hasło. Powinien także posiadać

mechanizmy pozwalające na określenie uprawnień użytkownika do korzystania z przetwarzanych informacji (np. prawo do odczytu danych, modyfikacji istniejących danych, tworzenia nowych danych, usuwania danych).

2. System informatyczny przetwarzający dane osobowe musi posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować:
- rozpoczęcie i zakończenie pracy przez użytkownika systemu,
- operacje wykonywane na przetwarzanych danych, a w szczególności ich dodanie, modyfikację oraz usunięcie,
- przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom nie będącym właścicielem ani współwłaścicielem systemu,
- nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,
- błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.

3. Zapis działań użytkownika uwzględnia:
- identyfikator użytkownika,
- datę i czas, w którym zdarzenie miało miejsce,
- rodzaj zdarzenia,
- określenie informacji, których zdarzenie dotyczy (identyfikatory rekordów).

4. W ramach możliwości technicznych system informatyczny powinien posiadać mechanizmy pozwalające na automatyczne powiadomienie Administratora danych lub osoby przez niego uprawnionej o zaistnieniu zdarzenia krytycznego (mogącego mieć krytyczne znaczenie dla bezpieczeństwa przetwarzanych danych osobowych).

5. System informatyczny powinien zapewnić zapis faktu przekazania danych osobowych z uwzględnieniem:
- identyfikatora osoby, której dane dotyczą,
- osoby przesyłającej dane,
- odbiorcy danych,
- zakresu przekazanych danych osobowych,
- daty operacji,
- sposoby przekazania danych.

§ 17. Usuwanie danych

1. Dane osobowe, dla których ustał cel przetwarzania, należy usuwać na bieżąco, na każdym etapie przetwarzania danych.

2. Dane, które zgodnie z obowiązującymi przepisami powinny podlegać archiwizacji, należy przekazać do archiwum.

3. Administrator danych raz do roku dokonuje przeglądu wszystkich zasobów danych osobowych w celu realizacji obowiązku ograniczenia celu przetwarzania oraz minimalizacji danych. Z przeglądu sporządzany jest raport.

§ 18. Zarządzanie zgodami na przetwarzanie danych osobowych

1. Zgoda na przetwarzanie danych osobowych musi spełniać warunki określone w RODO.

2. Pracownicy zobowiązani są do bieżącego i okresowego dokonywania przeglądu klauzul zgód, na podstawie których Administrator danych dokonuje przetwarzania danych osobowych pod kątem ich aktualności i zgodności z prawem.

3. Administrator danych weryfikuje, nie rzadziej niż raz do roku, czy przetwarzanie danych odbywa się na podstawie aktualnych i zgodnych z prawem zgód osób, których dane są przetwarzane.

§ 19. Zarządzanie obowiązkiem informacyjnym

1. Obowiązek informacyjny musi spełniać warunki określone w RODO.

2. Pracownicy zobowiązani są do bieżącego i okresowego dokonywania przeglądu klazul informacyjnych pod kątem ich aktualności i zgodności z prawem.

3. Administrator danych weryfikuje, nie rzadziej niż raz do roku, czy klauzule informacyjne są aktualne i zgodne z prawem.

§ 20. Ochrona danych w fazie projektowania

1. Wprowadza się obowiązek stosowania mechanizmów zapewniających zgodność z RODO na każdym etapie prac/działań związanych z przygotowaniem/projektowaniem prac zorientowanych do przetwarzania danych.

2. Ochrona danych w fazie projektowania jest uwzględniana w procesie analizy ryzyka sporządzanej przez Administratora danych.

§ 21. Domyślna ochrona danych

Wszystkie systemy, aplikacje, urządzenia, programy informatyczne, z których korzysta lub będzie korzystał w przyszłości Administrator danych muszą zapewniać domyślną ochronę danych osobowych.

§ 22. Umowy powierzenia przetwarzania danych

1. Projekt umowy powierzenia przetwarzania danych osobowych jest przygotowywany przez pracownika merytorycznego, odpowiedzialnego za proces powierzenia, i powinien uwzględniać wymagania określone w art. 28 RODO.

2. Projekt umowy jest przekazywany do zaopiniowania:
1) Inspektorowi Ochrony Danych;
2) Administratorowi systemów informatycznych - w przypadku gdy przedmiotem umowy są dane osobowe przetwarzane w systemach informatycznych.

3. Przed zawarciem umowy powierzenia przetwarzania danych osobowych nie można udostępniać podmiotowi danych osobowych.

§ 23. Procedury wykonania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.

2. Prace serwisowe dokonywane w obszarach przetwarzania danych u Administratora danych prowadzone w tym zakresie mogą być wykonywane wyłącznie przez pracowników Administratora danych lub przez upoważnionych przedstawicieli wykonawców zewnętrznych znajdujących się w towarzystwie pracowników Administratora danych. Przed rozpoczęciem prac serwisowych przez przedstawicieli wykonawców zewnętrznych konieczne jest potwierdzenie tożsamości tych osób.

3. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
- likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
- przekazanie podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
- naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez Administratora danych.

§ 24. Przetwarzanie danych poza obszarem przetwarzania

1. W przypadku przekazywania urządzeń lub nośników zawierających dane osobowe, w szczególności dane szczególnych kategorii, poza obszar przetwarzania danych, zabezpiecza się je w sposób zapewniający poufność, integralność i rozliczalność tych danych, przez co rozumie się:
- ograniczenie dostępu do danych osobowych hasłem zabezpieczającym dane przez osobami nieuprawnionymi,
- stosowanie metod kryptograficznych,
- stosowanie odpowiednich zabezpieczeń fizycznych,
- stosowanie odpowiednich zabezpieczeń organizacyjnych,

W zależności od stopnia zagrożenia zalecane jest stosowanie kombinacji wyżej wymienionych zabezpieczeń.

2. Dane osobowe przetwarzane na komputerach przenośnych powinny być zabezpieczone w sposób zapewniający poufność tych danych, w szczególności dane te powinny być zabezpieczone metodami kryptograficznymi.

§ 25. Zasady komunikacji w sieci teleinformatycznej

1. Przesyłanie danych osobowych drogą teletransmisji (w szczególności pocztą elektroniczną) powinno odbywać się wyłącznie przy wykorzystaniu wymaganych zabezpieczeń chroniących przed nieuprawnionym dostępem, w szczególności takich jak ochrona kryptograficzna.

2. Użytkownicy systemu przesyłający dane osobowe drogą teletransmisji powinni przed każdorazowym przesłaniem danych upewnić się, że stosowana jest ochrona kryptograficzna.

3. Inne technologie sieciowe, takie jak sieci lokalne, oparte na falach radiowych nie mogą być wykorzystywane do przekazu informacji, o ile połączenie nie jest szyfrowane. Takie połączenia mogą być używane jedynie dla wymiany poczty elektronicznej, o ile wiadomo, że nie zawiera ona danych osobowych.

4. ASI powinien chronić system przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem, poprzez:
- kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną,
- kontrolę działań inicjowania z sieci publicznej i systemu informatycznego.

Kontrola opisana powyżej powinna być dokumentowana przez osoby wykonujące te czynności.

§ 26. Zgodność

1. Niniejsza Polityka oraz dokumenty z nią powiązane powinny być aktualizowane wraz ze zmieniającymi się przepisami oraz zmianami faktycznymi u Administratora danych, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.

2. Okresowy przegląd Polityki oraz dokumentów powiązanych powinny mieć na celu stwierdzenie czy ich postanowienie odpowiadają aktualnej i planowanej działalności Administratora danych oraz są prawnie aktualne w momencie dokonywania przeglądu.

3. Powyższe zadania realizuje IOD.

§ 27. Postępowanie w przypadku naruszenia ochrony danych osobowych

1. Procedurę opisaną w niniejszym paragrafie stosuje się do przypadków naruszenia lub podejrzenia naruszenia ochrony danych osobowych przetwarzanych w Szkole.

2. Za okoliczność, które uznaje się za naruszenie lub podejrzenie naruszenia ochrony danych osobowych, uważa się w szczególności:
- nieuprawniony dostępnych lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują,
- nieuprawnione naruszenie lub próby naruszenia poufności, integralności i rozliczalności danych osobowych lub systemu teleinformatycznego,
- niezamierzoną zmianą lub utratę danych zapisanych na kopiach zapasowych,
- udostępnienie osobom trzecim danych osobowych lub ich części,
- wydarzenia losowe, obniżające poziom ochrony systemu,
- zagubienie lub kradzież sprzętu informatycznego lub nośników zewnętrznych zawierających dane osobowe.

3. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie ochrony danych osobowych pracownicy zobowiązani są do bezzwłocznego powiadomienia o tym fakcie Administratora danych oraz IOD, a w przypadku gdy naruszenie dotyczy danych przetwarzanych w systemie informatycznym – także ASI.

4. Do czasu przybycia IOD i ASI zgłaszający:
   - powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów,
   - zabezpiecza elementy systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osób trzecich,
   - podejmuje wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom.

5. IOD sporządza raport z przebiegu zdarzenia.

6. Po zaistnieniu incydentu, IOD odnotowuje ten fakt w ewidencji naruszeń i incydentów.

§ 28. Odpowiedzialność

Osoba, która:
- przetwarza dane osobowe do których przetwarzania nie jest uprawniona lub których przetwarzanie jest zabronione lub niezgodnie z celem przetwarzania,
- udostępnia dane osobowe lub umożliwia dostęp do nich osobom nieupoważnionym,
- nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o przysługujących jej prawach lub przekazania tej osobie informacji umożliwiających jej korzystanie z przysługujących jej praw,
- w inny sposób narusza ochronę danych osobowych,

podlega odpowiedzialności zgodnie z art. 52 kodeksu pracy.

DYREKTOR SZKOŁY
mgr Agnieszka Piskorek

Załącznik nr 1 do Polityki

POLECENIE PRZETWARZANIA DANYCH OSOBOWYCH

NR ..... / .....

Działając na podstawie art. 29 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)

wydaję Pani/Panu:

.....
(imię i nazwisko)

.....
(stanowisko służbowe)

polecenie przetwarzania danych osobowych.

Jest Pani/Pan upoważniona/upoważniony do przetwarzania danych osobowych wyłącznie w zakresie:

- wynikającym z Pani/Pana zadań służbowych określonych w Regulaminie Organizacyjnym ...., przypisanych do Pani/Pana referatu/samodzielnego stanowiska*,
- poleceń przełożonego*,
- realizacji obowiązków wynikających z zawartej umowy cywilno-prawnej*,
- realizacji obowiązków wynikających z umowy nr .... z dnia.....*

Upoważnienie jest ważne od dnia .....na czas/do* .....

W każdym przypadku upoważnienie traci ważność z chwilą ustania stosunku pracy lub wygaśnięciu umowy.

.....
(data i podpis Administratora Danych)

Odebrałem 1 egz.

.....
(data i podpis osoby upoważnionej)

---

* niepotrzebne skreślić

Załącznik nr 2 do Polityki

Ewidencja poleceń przetwarzania danych osobowych

Nr polecenia	Imię, nazwisko	data wydania polecenia	data cofnięcia polecenia	uwagi
1/2018				