załącznik nr 1
do Zarządzenia nr 19a/2018
z 25 maja 2018 r.

Polityka Ochrony Danych Osobowych w Zespole Szkół Ponadpodstawowych w Chojnie

I. Wstęp

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora danych w Zespole Szkół Ponadgimnazjalnych w Chojnie w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

II. Inwentaryzacja danych

1. Dane osobowe wymagające ochrony administrator danych opracował w wersji papierowej, stanowiącej załącznik nr 1 do Polityki Ochrony Danych.

2. Wykaz obejmuje zbiory ze stwierdzonym potencjalnym ryzykiem naruszenia praw lub wolności osób fizycznych.

3. Każdy ze zbiorów jest opisany w sposób umożliwiający przeprowadzenie analizy ryzyka.

4. W szkole została opracowana Polityka Zarządzania Ryzykiem w przetwarzaniu Danych Osobowych, określająca zasady szacowania skali ryzyka i prawdopodobieństwa jego wystąpienia.

5. Opis zbiorów obejmuje takie informacje, jak:

    1) nazwę zbioru;
    2) opis celów przetwarzania;
    3) charakter, zakres, kontekst, dokumentowane dane osobowe;
    4) odbiorcy;
    5) funkcjonalny opis operacji przetwarzania;

6) aktywa służące do przetwarzania danych osobowych (Informacje, Programy, systemy operacyjne, Infrastruktura IT, Infrastruktura, Pracownicy i współpracownicy, Outsourcing);
7) informacja o konieczności wpisu do rejestru czynności przetwarzania;
8) informacja o konieczności przeprowadzenia oceny skutków dla zbioru.

6. Administrator, w uzgodnieniu z Inspektorem Ochrony Danych, opracował karty zawierające analizę ryzyka dla poszczególnych operacji przetwarzania danych w zakresie aktywów biorących udział w przetwarzaniu danych.

III. Zapewnienie o przetwarzania danych osobowych zgodnie z prawem.

1. Administrator zapewnia, że:

   1) dane osobowe są przetwarzane legalnie na podstawie art. 6 i 9 RODO;

   2) zakres danych osobowych jest adekwatny do celów przetwarzania, z zachowaniem zasady minimalizacji danych;

   3) Administrator przechowuje dane osobowe przez konkretnie określony czas, z uwzględnieniem zasad określonych w Jednolitym rzeczowym wykazie akt, zatwierdzonym przez Archiwum Państwowe w Szczecinie;

   4) wobec osób, których dane są przetwarzane wykonano obowiązek informacyjny (art. 12, 13, 14 RODO) wraz ze wskazaniem im: prawa dostępu do danych osobowych, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, ‘bycia zapomnianym’;

   5) osoby, których dane osobowe są przetwarzane zostały poinformowane o funkcji IOD i przekazano dane kontaktowe;

   6) zapewniono ochronę danych osobowych w przypadku powierzenia danych w postaci umów powierzenia z podmiotami przetwarzającymi (art. 28 RODO).

2. Potwierdzenie przetwarzania danych osobowych zgodnie z prawem znajduje się w załączniku 1 – Wykaz Zbiorów Danych Osobowych.

3. Wzory klauzul informacyjnych znajdują się w załączniku 2 – Klauzule Informacyjne.

IV. Upoważnienia

1. Administrator odpowiada za nadawanie/anulowanie upoważnień do przetwarzania danych w zbiorach papierowych i systemach informatycznych.

2. Każda osoba upoważniona może przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa.

3. Upoważnienia nadawane są do zbiorów na wniosek przełożonych osób, które tego wymagają. Upoważnienia określają zakres operacji na danych.

4. Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności służbowych, udokumentowanego polecenia administratora w postaci umowy powierzenia.

5. Administrator prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych, załącznik 3 - Ewidencja osób upoważnionych.

V. **Procedura analizy ryzyka i ocena skutków**

1. Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń.

2. Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru danych osobowych lub grupy zbiorów charakteryzujących się podobieństwem celów i sposobów przetwarzania/ **odrębnie dla każdego zbioru.**

3. W przypadku konieczności przeprowadzenia oceny skutków (art. 35) wykonano następujące czynności:

   1) dokonano opisu planowanych operacji przetwarzania i celów przetwarzania – załącznik 4 – Wykaz zbiorów danych osobowych;

   2) określono zagrożenia we wszystkich aktywach biorących udział w procesie przetwarzania;

   3) dokonano oceny ryzyk, zgodnie z zasadami wskazanymi w Polityce Zarządzania Ryzykiem;

4) sporządzono mapę ryzyk ze wskazaniem istotności ryzyka;

   5) zaplanowano środki techniczne, organizacyjne i informatyczne dla ryzyk przekraczających istotność powyżej 4.

VI. **Instrukcja postępowania z incydentami**

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego lub Inspektora Ochrony Danych.
2. Do typowych podatności bezpieczeństwa danych osobowych należą:
   1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
   2) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;

3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
   1) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
   2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych);
   3) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

4. W przypadku stwierdzenia wystąpienia incydentu, Administrator lub IOD prowadzi postępowanie wyjaśniające w toku, którego:
   1) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki;
   2) proponuje ewentualne działania dyscyplinarne;
   3) proponuje działania na rzecz przywrócenia działań szkoły po wystąpieniu incydentu;
   4) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.

5. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze – załącznik 5 - Formularz rejestracji incydentu.

6. Zabrania się wywoływania incydentów przez osoby upoważnione do przetwarzania danych.

7. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w ciągu 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.

VII. **Regulamin Ochrony Danych**

Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania – załącznik 6 - Regulamin Ochrony Danych Osobowych.

Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania - załącznik 7 - Oświadczenie poufności.

VIII. **Procedura przywracania dostępności danych osobowych**

Zgodnie z art. 32 RODO, Administrator powinien zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego. Administrator opracował Procedury Przywracania Danych - załącznik 8 - Plan ciągłości działania

IX. **Wykaz zabezpieczeń**

1. Administrator prowadzi wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych. W wykazie wskazano stosowane zabezpieczenia proceduralne oraz zabezpieczenia jako środki techniczne, informatyczne i organizacyjne - załącznik 9 - Wykaz zabezpieczeń.

2. Wykaz jest aktualizowany po każdej analizie ryzyka

X. **Szkolenia**

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być poddana przeszkoleniu i zapoznana z przepisami RODO.

2. Za przeprowadzenie szkolenia odpowiada Administrator danych.

3. Administrator systematycznie szkoli pracowników szkoły.

4. Po przeszkoleniu z zasad ochrony danych osobowych, pracownicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.

5. Zgodnie z art. 32 RODO, Administrator będzie regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

załącznik nr 2
do Zarządzenia nr 19a/2018
z 25 maja 2018 r.

Regulamin Ochrony Danych Osobowych w Zespole Szkół Ponadgimnazjalnych w Chojnie

Spis treści:

Rozdział 1
Postanowienia ogólne

1. Regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych w Zespole Szkół Ponadgimnazjalnych w Chojnie zgodnie z RODO.

2. Regulamin obowiązuje wszystkich pracowników szkoły, podmioty przetwarzające dane osobowe na podstawie zawartych umów między przetwarzającym a powierzającym, użytkowników systemów informatycznych z dostępem do danych osobowych upoważnionych przez administratora na piśmie.

3. Każdy z wymienionych podmiotów jest zobowiązany do zapoznania się z dokumentem i bezwzględnego przestrzegania zawartych w nim zasad.

4. Administratorem danych osobowych w Zespole Szkół Ponadgimnazjalnych w Chojnie jest dyrektor szkoły.

5. Funkcje Inspektora Ochrony Danych sprawuje wyznaczona osoba.

Rozdział 2

Zasady korzystania z internetu

1. Użytkownik zobowiązany jest do korzystania z internetu wyłącznie w celach służbowych.

2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT i tylko w uzasadnionych przypadkach.

3. Użytkownik ponosi odpowiedzialność za szkody w infrastrukturze IT spowodowane przez oprogramowanie instalowane z Internetu.

4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo ze względu na zainstalowane na nich szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem.

5. Zabrania się w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.

6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą. W tej sytuacji należy „kliknąć" na ikonę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.

7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet, filtrowanie MAC-adresów.

Rozdział 3
Zasady korzystania z poczty elektronicznej

1. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do korzystania z poczty elektronicznej tylko w celach służbowych.

2. W przypadku przesyłania danych osobowych poza szkołę należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych dokumentów lub plików zzipowanych, podpis elektroniczny).

3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.

4. Każdy użytkownik przed wysłaniem poczty jest zobowiązany sprawdzić poprawność adresu odbiorcy dokumentu.

5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.

6. W celu ochrony przed zainfekowaniem komputera użytkownika i komputerów pracujących w sieci (kryptowirusy) zabrania się otwierania załączników (plików) w mailach nawet od prawdopodobnie znanych użytkownikowi nadawców bez weryfikacji nadawcy.

7. Zabrania się, bez weryfikacji wiarygodności nadawcy „klikać” na hiperlinki w mailach. Nieprzestrzeganie tej zasady może doprowadzić do zainfekowania komputera użytkownika i innych pracujących w sieci.
8. Wszystkie przypadki e-maili budzących podejrzenie należy zgłaszać administratorowi sieci/ informatykowi.

9. Przy wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW”. Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości”.

10. Zabrania się rozsyłania maili z tzw. „łańcuszkami szczęścia”. Adres mailowy prywatny służy wyłącznie do korespondencji służbowej.

11. Nakazuje się okresowe czyszczenie poczty z nieaktualnych e- mali i opróżnianie kosza.

12. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.

13. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.

14. Korzystanie z poczty elektronicznej dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.

15. Użytkownicy nie mają prawa korzystać z poczty elektronicznej w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub nietycznym i naruszającym cudzą godność i prywatność

16. Zabrania się dokonywanie w sieci zakupów, rezerwacji usług lub świadczeń na rzecz użytkownika z wykorzystaniem służbowej poczty elektronicznej.

17. Użytkownik, bez zgody Pracodawcy, nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy/Zleceniodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

18. Wszelkie dokumenty, opracowania, jak i inne treści przesyłane przez użytkownika podlegają zasadom ochrony prawa autorskiego i prawa własności przemysłowej, których użytkownik jest obowiązany przestrzegać.

Rozdział 4
Regulamin użytkowania komputerów przenośnych

1. Każdy Użytkownik komputera przenośnego winien zapoznać się z Regulaminem użytkowania komputerów przenośnych oraz pisemnie zobowiązać się do jego przestrzegania.

2. W przypadku przechowywania na komputerze przenośnym danych osobowych lub stanowiących tajemnicę Pracodawcy, Użytkownik zobowiązany jest do ich przechowywania na dysku szyfrowanym, zabezpieczonym co najmniej 8- znakowym hasłem (duże, małe litery, znaki specjalne lub cyfry).

3. Na komputerach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny, o ile jest to możliwe, znajdować się dane osobowe lub stanowiące tajemnicę Pracodawcy.

4. W przypadku kradzieży lub zgubienia komputera przenośnego, Użytkownik powinien natychmiast powiadomić o tym osobę odpowiedzialną za ochronę danych tj. Administratora Danych lub IOD, zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.

5. Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego w czasie transportu, a w szczególności:

   1) zaleca się przenoszenie go w specjalnym futerale;

   2) zabrania się pozostawiania komputera przenośnego w samochodzie podczas postoju w miejscu publicznym bez nadzoru;

   3) podczas jazdy samochodem zaleca się przechowywanie komputera przenośnego pod siedzeniem kierowcy.

6. W przypadku, gdy komputer przenośny pozostawiony jest w miejscu dostępnym dla osób nieupoważnionych, Użytkownik jest zobowiązany do stosowania kabla zabezpieczającego. W szczególności dotyczy to zabezpieczenia komputera na stanowisku pracy, podczas konferencji, prezentacji, szkoleń, targów itp.

7. W przypadku pozostawiania komputerów przenośnych w szkole zaleca się umieszczanie ich po zakończeniu pracy w zamykanych szafkach.

8. Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze lub na określonych nośnikach (pendrive, dysku zewnętrznym, CD, DVD). Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem osób niepowołanych.

9. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, Użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.

Rozdział 5
Zasady wynoszenia nośników z danymi osobowymi poza szkołę

1. Użytkownicy nie mogą wynosić poza szkołę bez zgody Administratora danych żadnych wymiennych elektronicznych nośników informacji, tj. wymienne twarde dyski, pendrive, płyty CD, DVD, pamięci typu Flash.

2. W sytuacjach koniecznych, za zgodą Administratora danych, wynoszone nośniki wymienne muszą być zaszyfrowane, a pliki opatrzone hasłem.

3. Zabrania się wynoszenia poza szkołę dokumentacji papierowej, zwierającej dane osobowe (dzienniki, arkusze ocen). W przypadku innej dokumentacji (prace klasowe, listy uczestników wycieczek, dokumentacja wycieczek) należy ją przenosić w zamykanych teczkach lub w innej bezpiecznej formie.

4. W przypadku przesyłania dokumentacji j/w należy korzystać z zaufanych firm kurierskich, za pokwitowaniem i w opakowaniach gwarantujących niedostępność osób trzecich.

Rozdział 6
Zasady zabezpieczania dokumentacji papierowej z danymi osobowymi

1. Upoważnieni pracownicy są zobowiązani do stosowania tzw. „**Polityki czystego biurka**”. Polega ona na zabezpieczaniu (zamykaniu) dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas nieobecności pracownika na stanowisku pracy w czasie pracy.
2. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach lub utylizacji ich w specjalnych bezpiecznych pojemnikach z przeznaczeniem do bezpiecznej utylizacji.
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach ogólnodostępnych.
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np., na terenach publicznych miejskich lub w lesie.

Rozdział 7
Zasady tworzenia kopii zapasowych

1. Zbiory danych osobowych w systemie informatycznych są zabezpieczane przed utratą lub uszkodzeniem za pomocą:
    1) urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej,
    2) sporządzania kopii zapasowych (kopie pełne).
2. Pełne kopie zapasowe zbiorów danych tworzone są 2 razy w ciągu roku. Kopie systemu kadrowego, płacowego i księgowego całościowe sporządzane są raz w miesiącu, a kopie przyrostowe raz dziennie.
3. W szczególnych sytuacjach, np. przed aktualizacją lub zmianą oprogramowania lub systemu należy wykonać bezwzględnie pełną kopię zapasową systemu.
4. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu. Za przeprowadzenie tych czynności odpowiada informatyk.
5. Nośniki danych po ustaniu ich użyteczności należy pozbawić danych lub zniszczyć w sposób uniemożliwiający odczyt danych.
6. Kopie całościowe przechowywane są przez 5 lat, a kopie przyrostowe przez 1 miesiąc.

Rozdział 8
Tworzenie kopii bezpieczeństwa dokumentacji serwera

1. Kopie zapasowe dokumentacji serwera tworzone są w sposób zautomatyzowany w oparciu o (specjalne oprogramowanie/wykorzystanie programowej funkcji serwera);
2. Kopie bezpieczeństwa sporządzane są także dla dokumentacji gromadzonej na dyskach stacji roboczych użytkowników w wybranym katalogu (np. w katalogu C:/Operacyjne/);

3. Kopie całościowe sporządzane są raz w miesiącu, a kopie przyrostowe raz dziennie;
4. Kopie sporządzane są na zewnętrznym twardym dysku, który przechowywany jest w szafie pancernej znajdującej się w sekretariacie szkoły;
5. Dodatkowo – raz w miesiącu sporządzane są całościowe kopie miesięczne na dysku zewnętrznym;
6. Dysk zewnętrzny jest opisany datą sporządzenia kopii;
7. Kopie całościowe przechowywane są przez okres 5 lat, a kopie przyrostowe przez 1 miesiąc;
8. Kopie przechowywane są w sejfie w sekretariacie szkoły;
9. Niszczenie dysku zewnętrznego odbywa się poprzez jego fizyczne zniszczenie.

Rozdział 9
Procedura niszczenia danych na nośnikach elektronicznych

1. W odniesieniu do nośników przenośnych (pendrive'y) oraz nośników danych zainstalowanych w komponentach informatycznych – złomowanych stosowane są mechanizmy bezpiecznego kasowania informacji:
    1) za pomocą specjalistycznego oprogramowania;
    2) przy użyciu demagnetyzacji;
    3) poprzez fizyczne niszczenie (pocięcie, spalenie itp.) nośników;
2. Wyznaczony administrator dokonuje kontroli prawidłowości usunięcia informacji.
3. Nośniki usuwalne, które nie mogą być ponownie wykorzystane, są niszczone.
4. Za właściwe skasowanie informacji zawartej na nośniku przenośnym lub w pamięci masowej stacji roboczej odpowiada użytkownik.
5. Za kasowanie informacji z pamięci masowych serwerów oraz nośników kopii archiwalnych i zapasowych odpowiada administrator danych.
6. Niszczenie nośnika zostaje odnotowane w protokole zniszczenia.

Rozdział 10
Procedura niszczenia danych na nośnikach papierowych

1. Dokumentacja papierowa niszczona jest w niszczarkach paskowych oraz w niszczarkach o podwyższonym standardzie.

Rozdział 11
Procedura napraw w serwisach zewnętrznych

1. Komputery przeznaczone do naprawy należy wysyłać bez dysków, a urządzenia mobilne bez kart pamięci.
2. W przypadku naprawy sprzętu z danymi osobowymi na nośniku należy je wpierw trwale usunąć z użyciem specjalistycznego oprogramowania.

3. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest zawarcie specjalnego zapisu w umowie serwisowej, gwarantującego bezpieczną naprawę (należy na to zwrócić uwagę przy zakupach sprzętu).
4. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest przekazywanie do naprawy uszkodzonego sprzętu z danymi zaszyfrowanymi na dysku/karcie pamięci. Sprzęt przekazywany jest do serwisu bez podawania hasła.
5. Rekomendowane jest korzystanie z serwisu, który dokonuje napraw u klienta (umowy gwarancyjne on-site).

Rozdział 12
Postępowanie dyscyplinarne

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.
2. Postępowanie sprzeczne z powyższymi zasadami może też być uznane przez Pracodawcę za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.

załącznik nr 3
do Zarządzenia nr 19a/2018
z 25 maja 2018 r.

Polityka Zarządzania Ryzykiem w procesie przetwarzania danych osobowych w Zespole Szkół Ponadgimnazjalnych w Chojnie

---

Rozdział 1
Postanowienia ogólne

§ 1.1. Ilekroć w dokumencie jest mowa o:

1) **administratorze danych** – należy przez to rozumieć Dyrektora Zespołu Szkół Ponadgimnazjalnych w Chojnie

2) **aktywach** – należy przez to rozumieć środki materialne i niematerialne mające wpływ na przetwarzanie danych;

3) **proces przetwarzania danych** – zespół operacji (czynności) wykonywanych na danych osobowych lub zestawach danych w celu określonego ich przetwarzania;

4) **operacji przetwarzania danych** – należy przez to rozumieć każdą czynność wykonywaną na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka, jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adoptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawniane poprzez wysłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

5) **ryzyku –** należy przez to rozumieć możliwość zaistnienia zdarzenia, które będzie miało wpływ na realizację założonych celów w zakresie ochrony danych osobowych. Ryzyko mierzone jest siłą skutku oddziaływania oraz prawdopodobieństwem jego wystąpienia;

6) **zarządzanie ryzykiem** – należy przez to rozumieć realizowany przez administratora danych osobowych proces, którego celem jest identyfikacja potencjalnych ryzyk, które mogą mieć wpływ na realizację celów i zadań jednostki;

7) **mapa ryzyka** – tabela (macierz) odzwierciedlająca ocenę siły oddziaływania i prawdopodobieństwo wystąpienia zidentyfikowanego ryzyka w placówce;

8) **ocena ryzyka** – należy przez to rozumieć czynność polegającą na porównaniu wyników uzyskanych podczas analizy ryzyka z kryteriami oceny ryzyka określonymi na etapie projektowania systemu bezpieczeństwa danych;

9) **kryteriach akceptacji ryzyka** – są to kryteria, które określają dopuszczalność ryzyka, zdefiniowane poprzez wartość progową. Akceptowaną wartością jest ryzyko tylko w zakresie 0 - 4, przy przyjętych 5-stopniowych skalach szacowania prawdopodobieństwa wystąpienia ryzyka i jego skutków;

10) **rejestr ryzyk** – należy przez to rozumieć dokument odzwierciedlający przeprowadzoną identyfikację i analizę ryzyk, a także przyjętą reakcję na ryzyko;

11) **bezpieczeństwie informacji** – zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;

12) **zdarzeniu związanym z bezpieczeństwem danych** – zdarzenie związane z bezpieczeństwem informacji, jako określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe naruszenie Polityki Bezpieczeństwa Informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem danych;

13) **incydencie** związanym z bezpieczeństwem danych – jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem danych osobowych, które stwarzają znaczne zakłócenia zadań i zagrażają bezpieczeństwu danych;

14) **zagrożeniu** – to wszystkie niekorzystne czynniki mogące przyczynić się w trakcie pracy z danymi osobowymi do wystąpienia incydentu, mogącego mieć wpływ na ich ujawnienie bądź utratę;

15) **podatność** – słabość, która może być wykorzystana przez zagrożenie, powodując niekorzystne skutki;

16) **dostępności** — należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w określonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym;

17) **integralności** — należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony;

18) **poufności** — należy przez to rozumieć właściwość określającą, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym;

19) **informatycznym nośniku danych** — należy przez to rozumieć materiał służący do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej;

20) **zasobach systemu teleinformatycznego** – należy przez to rozumieć informacje przetwarzane w systemie teleinformatycznym, jak również osoby, usługi, oprogramowanie, dane i sprzęt oraz inne elementy mające wpływ na bezpieczeństwo tych informacji;

Celem analizy ryzyka jest zastosowanie środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku wynikającemu z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

§ 2.1. Polityka zarządzania ryzykiem w zakresie ochrony danych osobowych, zwana dalej „polityką zarządzania ryzykiem”, obejmuje:

1) zakres zadań i obowiązków podmiotów uczestniczących w procesie zarządzania ryzykiem;
2) zasady i tryb identyfikacji ryzyka;
3) zasady i tryb dokonywania analizy ryzyka;
4) zasady określania właściwej reakcji na ryzyko.

§ 3. Polityka zarządzania ryzykiem ma zastosowanie dla wszystkich samodzielnych stanowisk wskazanych w Regulaminie Pracy.

§ 4. Zarządzanie ryzykiem jest procesem ciągłym i nie ogranicza się do działań określonych w § 2 ust. 1.

§ 5. Celem zarządzania ryzykiem jest zwiększenie prawdopodobieństwa osiągnięcia wyznaczonych celów i zadań w zakresie ochrony danych osobowych, poprzez ograniczenie prawdopodobieństwa wystąpienia ryzyka oraz zabezpieczanie się przed jego skutkami. Następuje to poprzez:

1) rozpoznanie, czyli identyfikowanie ryzyka, określenie rodzajów ryzyk, które wiążą się z działalnością placówki w zakresie ochrony danych osobowych i dokonywanie ich pomiaru;

2) ocenę ryzyka i jego istotności, przy pomocy skali określonej w § 9;

3) zarządzanie ryzykiem, które polega na badaniu efektywności i skuteczności podejmowanych działań, poprzez system kontroli instytucjonalnej i zewnętrznej;

4) kontrolę zarządzania ryzykiem, której istotą podjętych działań jest ocena zastosowanych metod redukcji ryzyka, prowadząca do skutecznego i efektywnego realizowania celów i nałożonych zadań.

Rozdział 2
Zakresy zadań i obowiązków

§ 6.1. Za realizację polityki zarządzania ryzykiem odpowiada Dyrektor szkoły poprzez:

1) kształtowanie i wdrażanie polityki zarządzania ryzykiem;
2) nadzór i monitorowanie skuteczności procesu zarządzania ryzykiem;
3) wyznaczanie poziomu akceptowalnego dla każdego ryzyka;
4) podejmowanie decyzji dotyczących sposobu reakcji na poszczególne ryzyka.

2. Pracownicy na samodzielnych stanowiskach odpowiadają za zarządzanie ryzykiem poprzez:

1) identyfikację ryzyk związanych z realizacją przydzielonych zadań w zakresie ochrony danych osobowych;
2) wskazywanie właścicieli zidentyfikowanych ryzyk;
3) przeprowadzanie analizy zidentyfikowanego ryzyka we współpracy z IOD;
4) proponowanie sposobu postępowania w odniesieniu do poszczególnych ryzyk;
5) wdrażanie działań zaradczych w stosunku do zidentyfikowanego ryzyka.

3. Pracownicy wymienieni w ust. 2 są zobowiązani do współpracy z dyrektorem szkoły.

Rozdział 3
Identyfikacja ryzyka

§ 7.1. Identyfikacja ryzyk prowadzona jest dla wszystkich zbiorów danych na poziomie jednostki i na poziomie poszczególnych samodzielnych stanowisk pracy stanowiącym załącznik nr 1 do Polityki Zarządzania Ryzykiem..

2. W procesie identyfikacji ryzyka uwzględnia się zagrożenia. Ze względu na ich źródło ryzyka dzielą się na:
1) zewnętrzne – rodzaj ryzyka determinowanego przez czynniki zewnętrzne;
2) wewnętrzne – ryzyko to obejmuje działania wewnętrzne placówki i może być zarządzane wewnątrz jednostki.

3. Każde zidentyfikowane ryzyko ujmuje się w rejestrze, stanowiącym załącznik nr 2 do Polityki Zarządzania Ryzykiem.

4. Dla każdego zidentyfikowanego ryzyka ustala się jego właściciela.

5. Każdy pracownik ma prawo i obowiązek zgłaszania swojemu bezpośredniemu przełożonemu ryzyk zidentyfikowanych podczas wykonywania przydzielonych zadań w zakresie ochrony danych osobowych.

Rozdział 4
Analiza ryzyka

§ 8.1. Każde ryzyko w zakresie ochrony danych osobowych podlega analizie pod kątem jego istotności na osiąganie celów i zadań. Istotność ryzyka jest iloczynem skali prawdopodobieństwa jego wystąpienia i wartości oszacowanych potencjalnych skutków.

2. Każde ryzyko jest oceniane pod względem prawdopodobieństwa jego wystąpienia i skutku oddziaływania.

3. W celu dokonania oceny ryzyka wykorzystuje się Mapę Ryzyka, którą stanowi macierz prawdopodobieństwo – skutek – załącznik nr 3 do Polityki Zarządzania Ryzykiem.

3. Mapa ryzyka definiuje ryzyka na:

1) niskie o wartości 4 i mniejszej;
2) średnie o wartości powyżej 4 i mniejszej niż 9;
3) wysokie – o wartości powyżej 9 i mniejszej niż 16.
4) katastrofalne – o wartości powyżej 16.

4. Przy ocenie prawdopodobnych skutków wystąpienia ryzyka przyjmuje się skalę punktową od 1 do 5, gdzie;

1) 1 – oznacza skutek nieznaczny;
2) 2 – oznacza skutek mały;
3) 3 – oznacza skutek średni;
4) 4 – oznacza skutek poważny;
5) 5 – oznacza skutek katastrofalny.

5. Przy ocenie prawdopodobieństwa wystąpienia ryzyka przyjmuje się skalę punktową od 1 do 5, gdzie:

1) 1 – oznacza prawdopodobieństwo rzadkie (0-20 %);
2) 2 – oznacza prawdopodobieństwo małe (21 - 40%);
3) 3 – oznacza prawdopodobieństwo możliwe(41 - 60 %);
4) 4 – oznacza prawdopodobieństwo prawdopodobne(61 - 80 %);
5) 5 – oznacza prawdopodobieństwo prawie pewne (81 -100 %).

Wskaźniki do punktacji oceny prawdopodobieństwa i skutków ryzyka określa załącznik nr 4 do Polityki Zarządzania Ryzykiem.

Rozdział 5
Reakcja na ryzyko

§ 9.1. Dla każdego istotnego zidentyfikowanego ryzyka właściciel ryzyka wskazuje optymalną reakcję. Przyjmuje się niżej wymienione reakcje na ryzyko:

1) tolerowanie – będzie to miało miejsce w przypadkach, kiedy koszty skutecznego przeciwdziałania ryzyku mogą przekraczać jego potencjalne korzyści, z zdolności do skutecznego przeciwdziałania są ograniczone lub wykraczające poza decyzje i działania wewnętrzne;

2) przeniesienie – dotyczyć to będzie kategorii ryzyk w odniesieniu do których nastąpi przeniesienie ich na inna instytucję, między innymi poprzez ubezpieczenie lub zlecenie usług na zewnątrz;

3) wycofanie się – dotyczyć to będzie grupy ryzyk dla których mimo podejmowanych działań nie udało się zmniejszyć ich istotności do akceptowanego poziomu;

4) przeciwdziałanie – dotyczyć to będzie kategorii ryzyk, które wymagać będą podjęcia zdecydowanych, przemyślanych i zaplanowanych działań prowadzących do ich likwidacji lub znacznego ograniczenia.

Rozdział 6
Postanowienia końcowe.

§ 11. 1. Strategia zarządzania ryzykiem obowiązuje od 25 maja 2018 roku.

2. Pracownicy szkoły obowiązani są do systematycznej analizy wystąpienia ryzyk na stanowiskach pracy i zgłaszania ich dyrektorowi szkoły.

……..……
dyrektor szkoły

załącznik nr 4
do Zarządzenia nr 19a/2018
z 25 maja 2018 r.

…… Chojna, ...

(imię i nazwisko)

……

(stanowisko)

OŚWIADCZENIE

o zachowaniu poufności
i zapoznaniu z przepisami

Ja, niżej podpisany/a oświadczam, iż zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań i obowiązków służbowych wynikających ze stosunku pracy, zarówno w czasie trwania umowy, jak i po jej ustaniu.

Oświadczam, że zostałem/am poinformowany/a o obowiązujących zasadach dotyczących przetwarzania danych osobowych, określonych w Polityce Ochrony Danych Osobowych, Regulaminie Ochrony Danych Osobowych oraz w Polityce Zarządzania Ryzykiem w procesie przetwarzania danych osobowych w Zespole Szkół Ponadgimnazjalnych w Chojnie i zobowiązuję się do ich przestrzegania. W szczególności oświadczam, że bez upoważnienia nie będę wykorzystywał/a danych osobowych ze zbiorów znajdujących się w Szkole.

Zostałem/am zapoznany/a z przepisami Ustawy o ochronie danych osobowych (Dz. U. 2018 r., poz. 1000) oraz Rozporządzeniem 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 (Dziennik Urzędowy UE - 4.5.2016 L 119/3) Poinformowano mnie również o grożącej, stosownie do przepisów Rozdziału 10 Ustawy o ochronie danych osobowych, odpowiedzialności cywilnej i postępowaniu przed sądem oraz Rozdziale 11 dotyczącym administracyjnych kar pieniężnych i przepisów karnych.

Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, ze złamanie zasad ochrony danych osobowych, obowiązujących w Zespole Szkół Ponadgimnazjalnych w Chojnie może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

……...
(podpis pracownika)