Szkoła Podstawowa nr 6
im. Jana Pawła II w Kraśniku
ul. Grunwaldzka 2, 23-204 Kraśnik
NIP: 715-10-20-547; REGON: 000783982
tel./fax 81 826 16 47
email: sp6krasnik@onet.pl

załącznik nr 3

do Zarządzenia nr 19 z dnia 2 września 2019 r.

Regulamin Ochrony Danych Osobowych

w Publicznej Szkole Podstawowej nr 6 im. Jana Pawła II w Kraśniku

Spis treści:

1. Postanowienia ogólne.
2. Polityką korzystania z internetu.
3. Polityką korzystania z poczty elektronicznej.
4. Polityka użytkowania komputerów przenośnych.
5. Polityka wynoszenia nośników elektronicznych poza szkołę.
6. Polityka zabezpieczania dokumentacji papierowej z danymi osobowymi.
7. Polityka tworzenia kopii zapasowych.
8. Polityka tworzenia kopii dokumentacji serwera.
9. Polityka niszczenia danych osobowych na nośnikach elektronicznych.
10. Polityka niszczenia danych na nośnikach papierowych.
11. Polityka naprawy sprzętu IT w serwisach zewnętrznych.
12. Odpowiedzialność dyscyplinarna.

Rozdział 1

Postanowienia ogólne

1. Regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych w Publicznej Szkole Podstawowej nr 6 im. Jana Pawła II w Kraśniku zgodnie z Rozporządzeniem PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.
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 Publicznej Szkole Podstawowej nr 6 im. Jana Pawła II w Kraśniku jest dyrektor szkoły.

Rozdział 2

Polityka 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.

Rozdział 3

Polityka 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 służbowy 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 oraz dokonywania bankowych z prywatnego konta.

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 przesyłane dokumentów, opracowania, jak i innych treści przesyłane przez użytkownika podlegają zasadom ochrony prawa autorskiego i prawa własności przemysłowej, które użytkownik jest obowiązany przestrzegać.

Rozdział 4

Polityka użytkowania komputerów przenośnych

1. Każdy Użytkownik komputera przenośnego winien zapoznać się z Regulaminem użytkowania komputerów przenośnych.

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 tylnym 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, 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

Polityka 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, pen-drive, 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

Polityka 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 ich nieobecności w trakcie godzin 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

Polityka 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, sporządzania kopii zapasowych (kopie pełne).

2. Pełne kopie zapasowe zbiorów danych tworzone są 2 razy w ciągu roku. Kopie systemu kadrowo płacowego 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
Polityka tworzenia kopii 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 wydzielonym twardym dysku wymiennym na komputerze w pomieszczeniu sekretariatu.

5. Dodatkowo – raz w miesiącu sporządzane są całościowe kopie miesięczne na streamerze.

6. Każda taśma streamera jest opisana datą jej sporządzenia.

7. Kopie całościowe przechowywane są przez okres 5 lat a kopie przyrostowe przez 1 miesiąc.

8. Kopie przechowywane są w sejfie w pomieszczeniu archiwum zakładowego.

9. Niszczenie streamera odbywa się poprzez jego rozmontowanie i zniszczenie taśmy poprzez jej pocięcie.

Rozdział 9

Polityka niszczenia danych osobowych na nośnikach elektronicznych

1. W odniesieniu do nośników przenośnych (pen-drive'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) 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

Polityka niszczenia danych na nośnikach papierowych

Dokumentacja papierowa niszczona jest w niszczarkach paskowych oraz w niszczarkach o podwyższonym standardzie/ Dokumentacja papierowa niszczona jest za pośrednictwem firmy niszczącej dokumenty. Firma zobowiązana jest do wykazania się bezpieczną procedurą utylizacji.

Rozdział 11

Polityka napraw sprzętu IT 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.

DYREKTOR SZKOŁY
Kuśmierz
mgr Monika Kusmierz

.....

(podpis dyrektora)