Załącznik Nr 1
do Zarządzenia Nr 1/2018/2019
Dyrektora Zespołu Szkół
im. Eugeniusza Kujana w Wierzawicach
z dnia 9 stycznia 2019 r.

INSTRUKCJA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Wierzawice, Listopad 2018 r

1. WSTĘP

Niniejszy dokument ma za zadanie stanowić zbiór zasad postępowania w zakresie ochrony danych osobowych. Został stworzony celem przedstawienia pracownikom i współpracownikom Szkoły uczestniczącym przy przetwarzaniu danych osobowych.

Pracownicy w ramach bieżącej pracy przestrzegają następujących zasad:

2. RUCH OSOBOWYCH

2.1. W pomieszczeniach gdzie zlokalizowany jest sprzęt komputerowy mogą przebywać wyłącznie osoby upoważnione. Osoby postronne (np. osoby odwiedzające Szkołę) mogą przebywać w tych pomieszczeniach wyłącznie pod nadzorem pracowników Szkoły.
2.2. Dostęp do pomieszczeń może być możliwy wyłącznie w czasie pracy.
2.3. Osoby wykonujące czynności konserwacyjne, naprawcze lub serwisowe, które nie posiadają upoważnienia mogą przebywać w obszarach bezpiecznych pod nadzorem osób upoważnionych.

3. ROZPOCZĘCIE I ZAKOŃCZENIE PRACY W POMIESZCZENIACH, W KTÓRYCH PRZETWARZA SIĘ INFORMACJE

3.1. Przed przystąpieniem do pracy w systemie informatycznym należy sprawdzić stację roboczą (komputer) i stanowisko pracy zwracając uwagę, czy nie zaszły okoliczności wskazujące na naruszenie lub próbę naruszenia bezpieczeństwa informacji powodowanych czynnikami zewnętrznymi (np. naruszenie zamków, krat, wybicie okna).
3.2. Przed wyjściem z pomieszczenia należy upewnić się, że okna oraz miejsca, w których przechowuje się informacje podlegające ochronie zostały zamknięte.
3.3. Po zamknięciu pomieszczenia należy odpowiednio zabezpieczyć klucze przed nieuprawnionym użyciem.

4. ZASADY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY W SYSTEMIE INFORMATYCZNYM

4.1. Przed uruchomieniem stacji roboczej tam gdzie jest to możliwe, należy upewnić się, że okablowanie jest odpowiednio podłączone i nie zostały uszkodzone gniazda prądowe.

4.2. Aby zawiesić pracę (tymczasowa przerwa w pracy w systemie informatycznym) należy zablokować stację kombinacją klawiszy „Microsoft + L". Dokumenty tradycyjne powinny zostać zabezpieczone zgodnie z polityką czystego biurka.
4.3. Kończąc pracę należy wylogować się z systemu informatycznego, zamknąć wszystkie aplikacje i upewnić się, że system operacyjny stacji roboczej zamknął się prawidłowo.

5. ROZMOWY TELEFONICZNE I FAKS

5.1. Pracownicy zobowiązani są do przestrzegania zakazu prowadzenia rozmów telefonicznych, podczas których może dochodzić do wymiany informacji chronionych, jeśli rozmowy te odbywają się w miejscach publicznych (np. pociągach, poczekalniach) oraz takich, które nie gwarantują zachowania poufności rozmów.
5.2. Pracownikom zabrania się zapisywania w systemach poczty głosowej informacji wrażliwych (tzn. takich, które są istotne i chronione na najwyższym poziomie).
5.3. Odczytanie indywidualnych wiadomości z faksów, automatycznych sekretarek lub systemów poczty głosowej powinno być możliwe wyłącznie po wprowadzeniu indywidualnego hasła.
5.4. W przypadku braku takiej możliwości urządzenia należy zabezpieczyć przed dostępem osób nieuprawnionych.
5.5. Przekazywanie za pomocą urządzeń faksowych dokumentów zawierających informacje chronione jest zabronione.

6. ZASADY TRANSMISJI PLIKÓW W SIECI TELEINFORMATYCZNEJ

6.1. Informacje o wysokiej istotności (np. dane osobowe), wysyłane poza sieć wewnętrzną muszą zostać zaszyfrowane.
6.2. Proponuje się wykorzystanie programów 7zip lub WinRar, które dają możliwość zaszyfrowania plików, które chcemy wysłać pocztą elektroniczną.
6.3. Hasło do zaszyfrowanego pliku należy przekazać SMS'em lub telefonicznie.
6.4. Jeżeli używany program do edycji tekstu (np. MS Word lub Excel) daje możliwość zaszyfrowania pliku hasłem – można skorzystać z tej funkcjonalności zamiast rozwiązania opisanego w punkcie 6.2.

7. BEZPIECZNA POCZTA ELEKTRONICZNA

7.1. Zaleca się korzystanie z poczty elektronicznej przeznaczonej do zastosowania biznesowego.
7.2. Nie zaleca się korzystania z darmowych kont pocztowych.
7.3. Nie zaleca się zapisywania haseł do poczty elektronicznej przez przeglądarkę internetową.
7.4. Podczas wysyłania wiadomości należy zweryfikować poprawność adresów e-mail odbiorcy.

7.5. Bezpieczne logowanie do poczty elektronicznej:
- 7.5.1. Jeśli logujesz się do swojego konta poprzez interfejs webmail, korzystając z przeglądarki internetowej, sprawdź jaki adres pojawia się w pasku adresu. Powinien rozpoczynać się https://.
- 7.5.2. Sprawdź certyfikat bezpieczeństwa (należy kliknąć kłódkę tuż obok paska adresu – wtedy wyświetla się informacja czy połączenie jest szyfrowane).
- 7.5.3. Jeżeli zarządzasz swoją pocztą elektroniczną włącz filtr antyspamowy.
- 7.5.4. Nie otwieraj załącznika, jeśli nie jesteś pewien, kto wysłał do Ciebie wiadomość.
- 7.5.5. Unikaj otwierania plików, które zawierają końcówkę: exe, .bat, .com, .lnk, .scr, .vbs.
- 7.5.6. Nie klikaj w linki od nieznanych nadawców, mogą zawierać przekierowanie do zainfekowanych stron.
- 7.5.7. Nie odpowiadaj na wiadomości od podejrzanych nadawców.
- 7.5.8. Korzystaj z dwuetapowego systemu uwierzytelniania, jeśli jest taka możliwość.
- 7.5.9. Jeśli uznasz wiadomość za niechcianą i podejrzaną, oznacz ją jako SPAM. Możesz to zrobić poprzez wciśnięcie przycisku „zgłoś SPAM". Umożliwia Ci to filtr antyspamowy. Możesz również dodać nadawcę do tzw. listy zablokowanych nadawców. W ten sposób uczysz swój filtr antyspamowy właściwej oceny swoich maili.
- 7.5.10. Do każdego konta podawaj zawsze inne hasło.

7.6. Korespondencja elektroniczna:
- 7.6.1. Pracownik przesyłając informacje za pośrednictwem poczty elektronicznej ponosi odpowiedzialność za prawidłowe zaadresowanie wiadomości elektronicznej i przesłanie jej do uprawnionego odbiorcy.
- 7.6.2. Zabrania się przesyłania za pośrednictwem poczty elektronicznej treści niezgodnych
- 7.6.3. z obowiązującymi przepisami prawa, naruszających zasady współżycia społecznego oraz naruszających prawa własności intelektualnej innych osób.
- 7.6.4. Zabrania się przesyłania do innych pracowników, wiadomości o treści niezwiązanej z jej działalnością, a w szczególności wiadomości elektronicznych zawierających m.in.: informacje o charakterze komercyjnym, niechcianych lub niepotrzebnych wiadomości.
- 7.6.5. Zabrania się rozsyłania za pośrednictwem poczty elektronicznej załączników zawierających pliki zagrażające lub mogące zagrażać bezpieczeństwu systemu teleinformatycznego Szkoły.
- 7.6.6. Zabrania się wykorzystywania przydzielonego pracownikowi służbowego konta pocztowego do celów prywatnych (np. prowadzenie korespondencji nie związanej z działalnością służbową, rejestrowania się przy użyciu konta służbowego na forach, portalach społecznościowych, newsletterach, itp.).

8. ZASADA CZYSTEGO EKRANU

8.1. Należy zadbać, aby ustawienia monitorów stacji roboczych nie pozwalały na przeglądanie wyświetlonych informacji osobom postronnym.
8.2. Zabrania się przechowywania istotnych plików i folderów na pulpicie. Zasada ta odnosi się w szczególności do wszelkiej dokumentacji zawierającej dane osobowe.

9. ZASADY STOSOWANIA HASEŁ

9.1. Rekomenduje się zmianę hasła co najmniej raz w każdym semestrze roku szkolnego.
9.2. Hasło powinno być złożone z minimum 8 znaków, dużych i małych liter, cyfr lub znaków specjalnych.
9.3. Nie dopuszcza się stosowania haseł zawierających: imiona i nazwiska, nazw pracownika, daty, nazw miast, regionów geograficznych, historycznych czy państw, wyrazów posiadających skojarzenie z osobą oraz prostych ciągów numerycznych (np. „123456" itp.).
9.4. Udostępnianie własnego hasła jest rażącym naruszeniem obowiązków pracowniczych.
9.5. Hasło nie powinno być zapisywane.
9.6. W przypadku podejrzenia, iż nasze hasło zostało ujawnione/skompromitowane (zostało zagubione, poznały je niepowołane osoby) należy bezzwłocznie zmienić hasło na nowe.
9.7. Niedopuszczalne jest stosowanie tych samych haseł prywatnie oraz w pracy.
9.8. W przypadku zablokowania hasła należy zwrócić się do informatyka w celu jego odblokowania.

10. ZASADY UŻYTKOWANIA SYSTEMÓW INFORMATYCZNYCH

10.1. Należy przywiązywać szczególną uwagę do weryfikacji poprawności danych przed ich wprowadzeniem do systemu. Wprowadzane dane powinny spełniać wymagania odnośnie jakości.
10.2. Wszelkie problemy z jakością oraz błędy w danych zauważone podczas przetwarzania danych należy niezwłocznie zgłaszać przełożonym lub rejestrować w systemie zgłoszeń incydentów, których te problemy dotyczą.
10.3. Należy postępować zgodnie z instrukcjami informatyka lub inspektora ochrony danych.

11. OPROGRAMOWANIE

10.1. Pracownik może korzystać jedynie z oprogramowania, na które pracodawca posiada aktualne licencje lub posiada prawo do używania.

10.2. Pracownik nie może za pomocą komputerów służbowych pobierać z Internetu lub przesyłać nielicencjonowanego oprogramowania oraz innych utworów chronionych prawem autorskim (w tym w szczególności utworów muzycznych, filmów, grafiki, gier komputerowych i tym podobnych).

10.3. Pracownik nie może instalować na komputerach pracodawcy prywatnych kopii oprogramowania, plików muzycznych i video, z żadnego nośnika i z żadnego innego urządzenia.

12. ZASADY DOTYCZĄCE DOSTĘPU DO SIECI INTERNET

12.1. Dostęp do sieci Internet może odbywać się wyłącznie na podstawie nadanych uprawnień w zakresie realizowania zadań służbowych. Korzystając z usług sieciowych należy przestrzegać następujących zasad:

12.1.1. użytkować Internet wyłącznie do celów służbowych,

12.1.2. korzystać wyłącznie z witryn internetowych niezbędnych do realizacji zadań służbowych,

12.1.3. zweryfikować certyfikaty udostępniane na witrynie,

12.1.4. pliki zawierające dane chronione należy przed wysłaniem zabezpieczyć (stosując szyfrowanie wiadomości z hasłem do otwarcia pliku).

12.2. Korzystaj z antywirusa i konta z ograniczonym uprawnieniami (nie admina).

13. W przypadku oznak zainfekowania komputera złośliwym oprogramowaniem należy:

13.1. Powiadomić Informatyka (zadanie pracownika).

13.2. Odłączyć komputer od sieci lokalnej oraz sieci Internet (zadanie Informatyka).

13.3. Jeśli nie można uruchomić komputera z dysku twardego (błąd przy starcie), należy spróbować uruchomić system w trybie awaryjnym lub przy użyciu dysku startowego systemu Windows (zadanie Informatyka).

13.4. Wykonać pełne skanowanie systemu operacyjnego (zadanie Informatyka).

14. Korzystanie z sieci Internet.

14.1. Pracownik ma prawo korzystać z sieci Internet wyłącznie: w celach związanych z realizacją zadań służbowych, zgodnie z obowiązującymi regulaminami i przepisami prawa, w zakresie przyznanych uprawnień.

14.2. Pracownikowi zabronione jest korzystanie z sieci Internet w celu: uzyskania nieuprawnionego dostępu do zasobów będących własnością Szkoły lub zasobów podmiotów zewnętrznych, pobierania,

udostępniania i rozpowszechniania jakichkolwiek materiałów (informacji, danych, tekstów, programów komputerowych, dźwięków, fotografii, grafik, filmów) naruszających prawa własności intelektualnej, pobierania, udostępniania i rozpowszechniania jakichkolwiek materiałów zakazanych przepisami prawa, w tym m.in. zawierających groźby, treści obraźliwe, zniesławiające, pornograficzne lub naruszających w jakikolwiek inny sposób prawa innych osób.

14.3. Zabronione jest podejmowanie przez pracowników działań powodujących istotne ograniczenia w korzystaniu z sieci Internet przez innych pracowników, a w szczególności: pobieranie dużej ilości danych, w sytuacji, gdy nie jest to uzasadnione wykonywanymi obowiązkami służbowymi, podejmowanie działań skutkujących ograniczeniami w funkcjonowaniu jakichkolwiek usług sieciowych.

14.4. Zabronione jest umożliwianie dostępu z Internetu do zasobów zlokalizowanych na urządzeniu komputerowym lub w sieci służbowej (np. przy wykorzystaniu serwerów WWW, ftp, programów tunelujących, P2P).

14. ZASADY KORZYSTANIA Z KOMPUTERÓW PRZENOŚNYCH

14.1. Pracownik może wynosić sprzęt komputerowy wyłącznie za zgodą dyrektora, po uprzednim upewnieniu się, że urządzenie zostało zaszyfrowane - np. poprzez ustanowienie hasła dostępu.

14.2. Komputer nie może być udostępniany osobom nieuprawnionym.

14.3. Instalacja oprogramowania może być dokonywana wyłącznie przez informatyka.

14.4. W przypadku kradzieży komputera należy o tym fakcie poinformować Dyrektora.

14.5. W razie utracenia urządzenia mobilnego – bez względu na to, czy był on szyfrowany, czy też nie – pracownik jest zobowiązany do poinformowania o tym Dyrektora.

14.6. Prywatne nośniki danych takie jak dysk zewnętrzny lub pendrive można wykorzystywać na komputerach służbowych pod warunkiem ich wcześniejszego zeskanowania przez program antywirusowy.

14.7. Komputery przenośne po zakończonej pracy winny być przechowywane w warunkach zapewniających ich bezpieczeństwo (np. szafy zamykane na klucz).

15. ZASADY DOTYCZĄCE POLITYKI ANTYWIRUSOWEJ

15.1. W przypadku, gdy program antywirusowy zgłasza nieaktualną bazę sygnatur wirusów należy o tym fakcie poinformować informatyka.

15.2. W przypadku identyfikacji wirusa na komputerze należy zawiesić pracę i niezwłocznie o tym fakcie poinformować informatyka.

15.3. Wszystkie nośniki zewnętrzne podłączane do stacji roboczej należy przed użyciem sprawdzić programem antywirusowym.

16. ZGŁASZANIE ZDARZEŃ MOGĄCYCH ŚWIADCZYĆ O NARUSZENIU BEZPIECZEŃSTWA

16.1. Wszystkie niestandardowe działania systemu informatycznego oraz zdarzenia mogące wskazywać na utratę bezpieczeństwa powinny być niezwłocznie zgłoszone informatykowi.

16.2. Symptomy wskazujące, na możliwość naruszenia bezpieczeństwa teleinformatycznego:

- obcy identyfikator w oknie logowania,
- nietypowe obciążenie (spowolnienie pracy) stacji roboczej,
- nowe oprogramowanie nieznanego typu,
- wyłączony program antywirusowy,
- zwiększona ilość niechcianej poczty (spamu),
- brak możliwości zalogowania się na własny identyfikator i hasło,
- nazwy plików w historii, które nie były otwierane,
- widoczne ślady przebywania osób trzecich w czasie nieobecności.

17. ZASADY NAPRAWY SPRZĘTU KOMPUTEROWEGO

17.1. W przypadku, gdy na nośnikach stanowiących integralną część sprzętu przekazywanego do naprawy, znajdują się informacje podlegające ochronie, pracownik ma obowiązek zgłosić ten fakt przy przekazywaniu urządzenia do serwisu. Sprzęt taki naprawiany jest pod nadzorem informatyka lub innego właściwego pracownika. Jeżeli zaś taki nadzór nie jest możliwy, to informacje muszą być uprzednio skutecznie usunięte, przy zapewnieniu możliwości ich późniejszego odtworzenia (np. przeniesienie na pendrive lub dysk zewnętrzny), bądź jeśli istnienie możliwość wymontowania nośnika danych (np. dysku twardego z komputera przenośnego), urządzenie należy przekazać do naprawy po uprzednim wymontowaniu nośnika. Fakt oddania urządzenia do naprawy stwierdza się poprzez spisanie protokołu zdawczo-odbiorczego.

17.2. Niedopuszczalny jest samodzielny serwis urządzenia komputerowego lub jego rozmontowywanie przez pracownika.

17.3. Pamiętaj, że takie same zagrożenia jakie generuje laptop, w większości przypadków dotyczą również telefonów komórkowych.

18. ZASADY MONITOROWANIA USŁUG I ZASOBÓW

18.1. Wszelkie usługi (np.: poczta elektroniczna, serwer plików, Internet), do których pracownik posiada dostęp, nie mogą być wykorzystywane do celów prywatnych ani działań, które stanowią naruszenie obowiązującego w Polsce prawa np. sabotaż, przestępstwa informatyczne, oszustwa, przemoc, rasizm, terroryzm itp.

18.2. Pracownik zobowiązany jest przechowywać kopie dokumentów istotnych dla funkcjonowania Szkoły w folderach sieciowych w celu zapewnienia możliwości objęcia ich procesem tworzenia kopii zapasowych. Dostęp do takich katalogów powinny mieć jedynie osoby uprawnione.
18.3. Informacje wrażliwe (np. dane osobowe, tajemnica przedsiębiorstwa) przesyłane pocztą elektroniczną poza siecią służbową winny być przesyłane w postaci zaszyfrowanej lub przesyłane w skompresowanym załączniku z użyciem hasła. Hasło powinno być przekazywane przy wykorzystaniu innego kanału komunikacji np. telefonicznie, przy pomocy wiadomości sms.
18.4. Komputery, konta pocztowe, nośniki danych – pamięci flash (pendrive) i inne urządzenia przekazane w ramach obowiązków służbowych, stanowią własność Szkoły i mogą być wykorzystywane wyłącznie w ramach realizacji powierzonych zadań związanych z wykonywaną pracą.
18.5. Wszelkie dane wytworzone przez pracowników na urządzeniach komputerowych należących do Szkoły są jej własnością.
18.6. Dyrektor oraz informatyk mają prawo i obowiązek kontrolować, czy pracownicy korzystający z urządzeń komputerowych stosują się do regulacji określonych w niniejszym dokumencie.

19. ZASADY ODPOWIEDZIALNOŚCI PRACOWNIKÓW ZA SZKODY ZWIĄZANE Z NIEPRAWIDŁOWYM UŻYTKOWANIEM URZĄDZEŃ SŁUŻBOWYCH

19.1. W przypadku uszkodzenia urządzenia komputerowego wynikającego z rażącego zaniedbania pracownika w zakresie sprawowania opieki nad powierzonym urządzeniem, pracownik ten może zostać obciążony kosztami jego naprawy bądź wymiany. Decyzję o obciążeniu kosztami naprawy, bądź odtworzenia sprzętu podejmuje Dyrektor.
19.2. Pracownicy naruszający zasady korzystania ze sprzętu komputerowego określone w niniejszym dokumencie, mogą podlegać odpowiedzialności na zasadach określonych w obowiązujących przepisach prawa.
19.3. Pracownicy ponoszą pełną odpowiedzialność za:
- powierzony sprzęt;
- naruszenie prywatności innego pracownika;
- dopuszczenie do infrastruktury teleinformatycznej osób nieuprawnionych;
- udostępnienie swojego komputera lub konta innej osobie oraz wykorzystanie przez nią dostępu do infrastruktury;
- podszywanie się pod innych pracowników;
- wszelkie dane przechowywane w ramach kont pocztowych;
- wszelkie dane przechowywane na komputerze służbowym podłączonym do sieci LAN oraz poczynania dokonywane za pomocą swojego komputera lub z wykorzystaniem swojego konta.