IV Liceum Ogólnokształcące
im. Henryka Sienkiewicza
Al. NMP 56, 42-200 Częstochowa
Tel. 34 324 16 14
NIP 573-10-33-040, IDS 000212682

Załącznik nr 21
do zarządzenia nr ...5... z dn. 30.09.2010....

Instrukcja bezpieczeństwa przetwarzania danych osobowych w IV LO im H. Sienkiewicza

§ 1. 1.Nadawanie uprawnień do przetwarzania danych oraz ich rejestrowanie w systemie informatycznym.

1) Do obsługi systemu informatycznego służącego do przetwarzania danych osobowych, może być dopuszczona wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych, wydane przez Administratora danych osobowych.
2) Upoważnienia do przetwarzania danych osobowych, o których mowa w punkcie 1.1. przechowywane są w teczkach akt osobowych pracowników oraz prowadzona jest ich ewidencja.
3) Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po :
   a) podaniu identyfikatora użytkownika i właściwego hasła w przypadku obsługi SIO, HERMES, BIP,
   b) podaniu właściwego hasła dostępu do stanowiska komputerowego w przypadku obsługi OFFICE, VULCAN.
4) Dla każdego użytkownika systemu informatycznego, który przetwarza dane osobowe, Administrator Bezpieczeństwa Informacji ustala niepowtarzalny identyfikator i hasło początkowe.
5) Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego, nie powinien być przydzielany innej osobie.
6) W przypadku utraty przez daną osobę uprawnień do dostępu do danych osobowych w systemie informatycznym. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, należy niezwłocznie wyrejestrować z systemu informatycznego, unieważnić jej hasło, oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych. Za realizację procedury rejestrowania i wyrejestrowywanie użytkowników w systemie informatycznym odpowiedzialny jest Administrator Bezpieczeństwa Informacji.

§ 2. 1. Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.

1) Dane osobowe przetwarzane są z użyciem dedykowanych serwerów, komputerów stacjonarnych.
2) Hasło użytkownika powinno mieć minimum 8 znaków i być zmieniane w przypadku :
   a) Systemu SIO, HERMES – co 30 dni,
   b) OFFICE, VULCAN, BIP – zmiana hasła dostępu do stanowiska komputerowego co 90 dni.
3) Hasło oprócz znaków małych i dużych liter winno zawierać ciąg znaków alfanumerycznych i specjalnych;

4) Hasła wpisywane z klawiatury nie mogą pojawiać się na ekranie monitorów w formie jawnej;
5) Hasło nie może zawierać żadnych informacji, które można kojarzyć z użytkownikiem komputera np. osobiste dane użytkownika, tj. nazwisko, inicjały, imiona, marka lub nr rejestracyjny samochodu itp.;
6) Hasło nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych. Użytkownik nie może udostępnić swojego identyfikatora oraz hasła jak również dostępu do stanowiska roboczego po uwierzytelnieniu w systemie osobom nieuprawnionym ani żadnej osobie postronnej;
7) Hasło użytkownika, umożliwiające dostęp do systemu informatycznego, należy utrzymywać w tajemnicy, również po upływie jego ważności;
8) Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi;
9) Hasła są zdeponowane w kasie pancernej w siedzibie dyrektora szkoły.
10) W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest do natychmiastowej zmiany hasła, lub w razie problemów powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji.

§ 3. 1. Procedury rozpoczęcia, zawieszenia i zakończenia pracy.

1) Dane osobowe, których administratorem jest IV LO mogą być przetwarzane sposobem tradycyjnym lub z użyciem systemu informatycznego tylko na potrzeby realizowania zadań statutowych i organizacyjnych szkoły;
2) Rozpoczęcie pracy użytkownika w systemie informatycznym następuje po poprawnym uwierzytelnieniu (zalogowaniu się do systemu);
3) Rozpoczęcie pracy w aplikacji musi być przeprowadzone zgodnie z instrukcją zawartą w dokumentacji aplikacji;
4) Zakończenie pracy użytkownika następuje po poprawnym wylogowaniu się z systemu oraz poprzez uruchomienie odpowiedniej dla danego systemu opcji jego zamknięcia zgodnie z instrukcją zawartą w dokumentacji;
5) Niedopuszczalne jest zakończenie pracy w systemie bez wykonania pełnej i poprawnej operacji wylogowania z aplikacji i poprawnego zamknięcia systemu;
6) Monitory stanowisk komputerowych znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych, a na których przetwarzane są dane osobowe należy ustawić w taki sposób, aby uniemożliwić osobom postronnym wgląd w dane;
7) Użytkownik ma obowiązek wylogowania się w przypadku zakończenia pracy. Stanowisko komputerowe nie może pozostać z uruchomionym i dostępnym systemem bez nadzoru pracującego na nim pracownika;
8) Wydruki zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym ich odczytanie przez osoby postronne. Wydruki nieprzydatne należy zniszczyć w stopniu uniemożliwiającym ich odczytanie w niszczarce dokumentów;
9) Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na obszarze, w którym są przetwarzane dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania;
10) Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać, na czas nieobecności osób zatrudnionych, w sposób uniemożliwiający dostęp do nich osobom trzecim;
11) Użytkownik niezwłocznie powiadamia Administratora Bezpieczeństwa Informacji w przypadku podejrzenia fizycznej ingerencji w przetwarzane dane osobowe lub użytkowane narzędzia programowe lub sprzętowe. Wówczas, użytkownik jest zobowiązany do natychmiastowego wyłączenia sprzętu.

§ 4. 1. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi do ich przetwarzania.

1) Zbiory danych osobowych w systemie informatycznym są zabezpieczane przed utratą lub uszkodzeniem za pomocą:
   a) urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej,
   b) sporządzanie kopii zapasowych (kopie pełne).
2) Pełne kopie zapasowe zbiorów danych tworzone są 2 razy w ciągu roku;
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 Administrator Bezpieczeństwa Informacji;
5) Nośniki danych po ustaniu ich użyteczności należy pozbawić danych lub zniszczyć w sposób uniemożliwiający odczyt danych.

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

1) Okresowe kopie zapasowe wykonywane są na płytach CD lub innych elektronicznych nośnikach informacji. Kopie zapasowe przechowuje się w sposób uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie w kasie pancernej pomieszczeniu dyrektora szkoły.

2) Dostęp do nośników z kopiami zapasowymi systemu oraz kopiami danych osobowych, ma wyłącznie Administrator Bezpieczeństwa Informacji .

3) Kopie miesięczne przechowuje się przez okres 6 miesięcy. Wykonywane co pół roku pełne kopie systemu kadrowego przechowuje się przez 50 lat. Kopie zapasowe należy bezzwłocznie usuwać po ustaniu ich użyteczności.

4) Usunięcie danych z systemu powinno zostać zrealizowane przy pomocy oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika informacji.

5) W przypadku kopii zapasowych sporządzanych indywidualnie przez użytkownika odpowiedzialnością za ich zniszczenie obarczony jest użytkownik.

6) W przypadku nośników informacji, przez ich zniszczenie rozumie się ich trwałe i nieodwracalne zniszczenie fizyczne do stanu nie dającego możliwości ich rekonstrukcji i odzyskania danych.

§ 6. 1.Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1) W związku z istnieniem zagrożenia dla zbiorów danych osobowych, ze strony wirusów komputerowych, których celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, konieczna jest ochrona sieci komputerowej i stanowisk komputerowych.

2) Wirusy komputerowe mogą pojawić się systemach szkoły poprzez: Internet, nośniki informacji takie jak: płyty CD, dyski przenośne, itp.

3) Przeciwdziałanie zagrożeniom ze strony wirusów komputerowych realizowane jest następująco:
   a) Komputer z dostępem do Internetu musi być zabezpieczony za pomocą oprogramowania antywirusowego.
   b) Zainstalowany program antywirusowy powinien być tak skonfigurowany, by co najmniej raz w tygodniu dokonywał aktualizacji bazy wirusów oraz co najmniej raz w tygodniu dokonywane było automatycznie sprawdzenie komputera pod kątem obecności wirusów komputerowych.
   c) Elektroniczne nośniki informacji takie jak dyski przenośne, należy każdorazowo sprawdzać programem antywirusowym przed użyciem, po zainstalowaniu ich w systemie. Czynność powyższą realizuje użytkownik systemu. W przypadku problemów ze sprawdzeniem zewnętrznego nośnika danych użytkownik jest zobowiązany zwrócić się z tym do Administratora Bezpieczeństwa Informacji.
   d) Komputery i systemy pracujące muszą mieć zainstalowany program antywirusowy a w przypadku komputerów z dostępem do Internetu, również posiadać oprogramowanie i mechanizmy zabezpieczające przed nieautoryzowanym dostępem z sieci (firewall).
   e) W przypadku, gdy użytkownik stanowiska komputerowego zauważy komunikat oprogramowania zabezpieczającego system wskazujący na zaistnienie zagrożenia lub rozpozna tego typu zagrożenie, zobowiązany jest zaprzestać jakichkolwiek czynności w systemie i niezwłocznie skontaktować się z Administratorem Bezpieczeństwa Informacji.
   f) Przy korzystaniu z poczty elektronicznej należy zwrócić szczególną uwagę na otrzymywane załączniki dołączane do treści wiadomości. Zabrania się otwierania załączników i wiadomości poczty elektronicznej od „niezaufanych" nadawców.
   g) Zabrania się użytkownikom komputerów, wyłączania, blokowania odinstalowywania programów zabezpieczających komputer (skaner antywirusowy, firewall) przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem.

§ 7. Udostępnianie danych osobowych i sposób odnotowania informacji o udostępnionych danych

7.1.Udostępnienie danych instytucjom może odbywać się wyłącznie na pisemny uzasadniony wniosek lub zgodnie z przepisami prawa (OKE, CKE, Urząd Miasta, itp.).

§ 8. Wykonywanie przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych

8.1. Przeglądy i konserwacje systemu oraz zbiorów danych wykonuje Administrator Bezpieczeństwa Informacji na bieżąco.

8.2. Administrator Bezpieczeństwa Informacji okresowo sprawdza możliwość odtworzenia danych z kopii zapasowej.

8.3. Umowy dotyczące instalacji i konserwacji sprzętu należy zawierać z podmiotami, których kompetencje nie budzą wątpliwości, co do wykonania usługi oraz których wiarygodność finansowa zostały sprawdzone na rynku.

8.4. Naprawy sprzętu należy zlecać podmiotom, których kompetencje nie budzą wątpliwości, co do wykonania usługi. Naprawa sprzętu, na którym mogą znajdować się dane osobowe powinna odbywać się pod nadzorem osób użytkujących sprzęt oraz Administratora Bezpieczeństwa Informacji w miejscu jego użytkowania.

8.5. W przypadku konieczności naprawy poza miejscem użytkowania, sprzęt komputerowy, przed oddaniem do serwisu, powinien być odpowiednio przygotowany. Dane należy zarchiwizować na nośniki informacji, a dyski twarde, bezwzględnie, wymontować na czas naprawy.

8.6. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji, może być dokonana tylko za wiedzą i zgodą Administratora Bezpieczeństwa Informacji.

§ 9. Ustalenia końcowe

9.1. Osobom korzystającym z systemu informatycznego, w którym przetwarzane są dane osobowe w szkole zabrania się:

1) ujawniania loginu i hasła współpracownikom i osobom z zewnątrz,

2) pozostawiania haseł w miejscach widocznych dla innych osób,

3) udostępniania stanowisk pracy wraz z danymi osobowymi osobom nieuprawnionym,

4) udostępniania osobom nieuprawnionym programów komputerowych zainstalowanych w systemie,

5) używania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna,

6) przenoszenia programów komputerowych, dysków twardych z jednego stanowiska na inne,

7) kopiowania danych na nośniki informacji, kopiowania na inne systemy celem wynoszenia ich poza szkołę,

8) samowolnego instalowania i używania jakichkolwiek programów komputerowych w tym również programów do użytku prywatnego; programy komputerowe instalowane są przez Administratora Bezpieczeństwa Informacji,

9) używania nośników danych udostępnionych przez osoby postronne,

10) przesyłania dokumentów i danych z wykorzystaniem konta pocztowego prywatnego (niesłużbowego),

11) otwierania załączników i wiadomości poczty elektronicznej od nieznanych i „niezaufanych" nadawców,

12) używania nośników danych niesprawdzonych, niewiadomego pochodzenia lub niezwiązanych z wykonywaną pracą; w przypadku konieczności użycia niesprawdzonych przenośnych nośników danych, należy zgłosić te nośniki, w celu sprawdzenia - przeskanowania programem antywirusowym, Administratorowi Bezpieczeństwa Informacji,

13) tworzenia kopii zapasowych niechronionych hasłem i/lub bez odpowiednich zabezpieczeń miejsca ich przechowywania.

9.2. Ponadto zabrania się:

1) wyrzucania dokumentów zawierających dane osobowe bez uprzedniego ich trwałego zniszczenia,
2) pozostawiania dokumentów, kopii dokumentów zawierających dane osobowe w drukarkach, kserokopiarkach,
3) pozostawiania kluczy w drzwiach, szafach, biurkach, zostawiania otwartych pomieszczeń, w których przetwarza się dane osobowe,
4) pozostawiania bez nadzoru osób trzecich przebywających w pomieszczeniach szkoły, w których przetwarzane są dane osobowe,
5) pozostawiania dokumentów na biurku po zakończonej pracy, pozostawiania otwartych dokumentów na ekranie monitora bez blokady konsoli,
6) ignorowania nieznanych osób z zewnątrz poruszających się w obszarze przetwarzania danych osobowych,
7) przekazywania informacji będącymi danymi osobowymi osobom nieupoważnionym,
8) ignorowania zapisów Polityki Bezpieczeństwa szkoły.

9.3. Konieczne jest:

1) posługiwanie się własnym loginem i hasłem w celu uzyskania dostępu do systemów informatycznych,
2) tworzenia haseł trudnych do odgadnięcia dla innych,
3) traktowanie konta pocztowego szkoły jako narzędzia pracy i wykorzystywanie go jedynie w celach służbowych,
4) nie przerywanie procesu skanowania przez program antywirusowy na komputerze,
5) wykonywanie kopii zapasowych danych przetwarzanych na stanowisku komputerowym,
6) zabezpieczenie sprzętu komputerowego przed kradzieżą lub nieuprawnionym dostępem do danych.

9.4. Wszelkie przypadki naruszenia niniejszej Instrukcji należy zgłaszać Administratorowi Bezpieczeństwa Informacji lub bezpośredniemu przełożonemu.

§ 10. Zalecenia w zakresie przetwarzania danych osobowych sposobem tradycyjnym

1) Miejscem tworzenia, uzupełniania, przechowywania dokumentacji dotyczącej przetwarzania danych osobowych sposobem tradycyjnym są pomieszczenia w szkole: sekretariat, pokój nauczycielski, gabinet dyrektora, pedagoga, biblioteka.
2) Osoby prowadzące dokumentację zobowiązane są do zachowania tajemnicy służbowej.
3) Dokumentacji, o której mowa w punkcie 1.1. nie można wynosić poza teren szkoły.
4) Dokumentację, o której mowa w punkcie 1.1. archiwizuje się zgodnie z Instrukcją kancelaryjną.
5) Osoby prowadzące dokumentację zobowiązane są do niezwłocznego poinformowania Pełnomocnika dyrektora ds. przetwarzania danych osobowych o podejrzeniu dostępu do dokumentacji przez osoby nieupoważnione.

§ 11. Obowiązki Administratora Danych

1. Administrator danych zobowiązany jest do zapewnienia, aby dane osobowe były:

a) przetwarzane zgodnie z prawem,
b) zbierane dla oznaczonych, zgodnych z prawem celów,
c) merytorycznie poprawne i adekwatne w stosunku do celów.

2. Wyznacza osobę, zwaną dalej Administratorem Bezpieczeństwa Informacji, odpowiedzialnym za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.
3. Opracowuje instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych, przeznaczoną dla osób zatrudnionych przy przetwarzaniu tych danych.
4. Określa budynki, pomieszczenia lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego.
5. Opracowuje instrukcję, określającą sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.
6. Prowadzi ewidencję osób uprawnionych do przetwarzania danych osobowych w poszczególnych systemach.
7. Organizuje szkolenia mające na celu zaznajomienie każdej osoby przetwarzającej dane osobowe z przepisami dotyczącymi ich ochrony.
8. Odpowiada za to by zakres czynności osoby zatrudnionej przy przetwarzania danych osobowych określał odpowiedzialność tej osoby za:
   a) ochronę danych przed niepowołanym dostępem,
   b) nieuzasadnioną modyfikację lub zniszczenie danych,
   c) nielegalne ujawnienie danych.
   w stopniu odpowiednim do zadań realizowanych w procesie przetwarzania danych osobowych.

§ 12. Obowiązki Administratora Bezpieczeństwa Informacji

1. Nadzór na przestrzeganiem instrukcji określającej sposób zarządzania systemem informatycznym.
2. Nadzór nad właściwym zabezpieczeniem sprzętu oraz pomieszczeń, w których przetwarzane są dane osobowe.
3. Nadzór na wykorzystywany w szkole oprogramowaniem oraz jego legalnością.
4. Przeciwdziałanie dostępowi osób niepowołanych do systemu, w których przetwarzane są dane osobowe.
5. Podejmowanie odpowiednich działań w celu właściwego zabezpieczenia danych.
6. Badanie ewentualnych naruszeń w systemie zabezpieczeń danych osobowych.
7. Podejmowanie decyzji o instalowaniu nowych urządzeń oraz oprogramowania wykorzystywanego do przetwarzania danych osobowych.
8. Nadzór na naprawami, konserwacją oraz likwidacją urządzeń komputerowych zawierających dane osobowe.
9. Definiowanie użytkowników i haseł dostępu.
10. Aktualizowanie oprogramowania antywirusowego i innego, chyba że aktualizacje te wykonywane są automatycznie.
11. Nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności.
12. Wdrożenie szkoleń z zakresu przepisów dotyczących ochrony danych osobowych oraz środków technicznych i organizacyjnych przy przetwarzaniu danych w systemach informatycznych.
13. Sporządzanie raportów z naruszenia bezpieczeństwa systemu informatycznego.

Dyrektor Szkoły
mgr Jadwiga Sipa