INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

w Zespole Szkół Technicznych im. gen. Władysława Andersa w Białymstoku

AdministratorBezpieczeństwa Informacji

Białystok, 2014r.

S P I S T R E Ś C I

I. POSTANOWIENIA OGÓLNE

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2014 r. poz. 1182) oraz rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024) nakłada na administratora danych osobowych następujące obowiązki:

- zapewnienie bezpieczeństwa i poufności danych, w tym zabezpieczenie ich przed ujawnieniem,
- zabezpieczenie danych przed nieuprawnionym dostępem,
- zabezpieczenie danych przed udostępnieniem osobom nieupoważnionym(nieuprawnionym pozyskaniem),
- zabezpieczenie przed utratą danych,
- zabezpieczenie przed uszkodzeniem lub zniszczeniem danych oraz przed ich nielegalną modyfikacją.

Ochronie podlegają dane osobowe niezależnie od formy przechowywania, sprzęt komputerowy, systemy operacyjne i informatyczne oraz pomieszczenia, w których odbywa się proces przetwarzania.

Instrukcja określa ramowe zasady właściwego zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i system informatyczny, odpowiednie do zagrożeń i kategorii danych objętych ochroną.

II. PRZEZNACZENIE, DEFINICJE

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Zespole Szkół Technicznych im. gen. Władysława Andersa w Białymstoku, zwana dalej instrukcją – określa sposób zarządzania oraz zasady administrowania systemem informatycznym służącym do przetwarzania danych osobowych.

Ilekroć w instrukcjijest mowa o:

1) **Szkole**–rozumie się przez to **Zespół Szkół Technicznych im. gen. Władysława Andersa w Białymstoku**;
2) **administratorze danych osobowych**–rozumie się przez to Dyrektora Szkoły;
3) **danych osobowych**–rozumie się przez tokażdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby;

4) **zbiorze danych osobowych**–rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie;

5) **przetwarzaniu danych**–rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

6) **usuwaniu danych**–rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

7) **administratorze bezpieczeństwa informacji (ABI)**–rozumie się przez to osobę wyznaczoną przez Administratora Danych Osobowych, odpowiedzialną 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 wypadku naruszeń w systemie zabezpieczeń. Osoba ta odpowiedzialna jest również za nadzorowanie i poprawną pracę powierzonego mu sprzętu sieciowego oraz systemu operacyjnego w danej jednostce organizacyjnej, w tym w szczególności:
   - ma prawo do zmiany uprawnień wszystkich użytkowników,
   - za pomocą platformy zarządzania dysponuje bezpośrednio wszystkimi zasobami podległej mu sieci,
   - pełni kontrolę nad dostępem użytkowników do systemów,
   - podejmuje samodzielnie lub na polecenie Administratora Danych Osobowych odpowiednie działania w wypadku naruszeń w systemie zabezpieczeń;

8) **administratorze aplikacji**–rozumie się przez to osobę odpowiedzialną w danej jednostce organizacyjnej za bezpieczeństwo przetwarzania danych w ramach aplikacji, w tym administrującą prawami dostępu w ramach tej aplikacji;

9) **użytkownikach systemu**– rozumie się przez to osoby upoważnione do przetwarzania danych osobowych w systemie informatycznym;

10) **obszarze kontrolowanym**– należy przez to rozumieć obszar znajdujący się pod ochroną, o ograniczonym dostępie osób nieautoryzowanych, w którym odbywa się przetwarzanie danych,w tym danych osobowych.

Niniejsza Instrukcja zarządzania systemem informatycznym określa:

a) poziom bezpieczeństwa przetwarzania danych osobowych w systemieinformatycznym;

b) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym;

c) stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem;

d) sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz osoby odpowiedzialne za te czynności;

e) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;

f) metody i częstotliwość tworzenia kopii awaryjnych;

g) metody i częstotliwość sprawdzania obecności wirusów komputerowych oraz metody ich usuwania;

h) sposób, miejsce i okres przechowywania:

- elektronicznych nośników informacji zawierających dane osobowe,
- kopii zapasowych;

i) sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych;

j) sposób postępowania w zakresie komunikacji w sieci komputerowej;

k) procedury wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych.

III. OKREŚLENIE POZIOMU BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMIE INFORMATYCZNYM

1. Z analizy zagrożeń wynika, że w Szkole miejscami najbardziej zagrożonymi są pomieszczenia budynku, w których znajdują się zbiory danych osobowych gromadzone w kartotekach oraz urządzeniach służących do przetwarzania tych danych, do których mogą mieć nieuprawniony dostęp osoby nieupoważnione spoza Szkoły.
2. Do innych zagrożeń, na które może być narażone przetwarzanie danych osobowych w formie tradycyjnej należy zaliczyć:
   - oszustwo, kradzież, sabotaż;
   - zdarzenia losowe (powódź, pożar);
   - zaniedbania pracowników szkoły (niedyskrecja, udostępnienie danych osobie nieupoważnionej);
   - niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania;
   - pokonanie zabezpieczeń fizycznych;
   - podsłuchy, podglądy;
   - ataki terrorystyczne;
   - brak rejestrowania udostępniania danych;
   - niewłaściwe miejsce i sposób przechowywania dokumentacji
3. Do innych zagrożeń, na które może być narażone przetwarzanie danych

osobowych w systemach informatycznych należy zaliczyć:

- nie przydzielenieużytkownikom systemu informatycznego identyfikatorów;
- niewłaściwa administracja systemem;
- niewłaściwa konfiguracja systemu;
- zniszczenie (sfałszowanie) kont użytkowników;
- kradzież danych kont;
- pokonanie zabezpieczeń programowych;
- zaniedbania pracowników szkoły (niedyskrecja, udostępnienie danych osobie nieupoważnionej);
- niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania;
- zdarzenia losowe (powódź, pożar);
- niekontrolowane wytwarzanie i wypływ danych poza obszar przetwarzania z pomocą nośników informacji i komputerów przenośnych;
- naprawy i konserwacje systemu lub sieci teleinformatycznej wykonywane przez osoby nieuprawnione;
- przypadkowe bądź celowe uszkodzenie systemów i aplikacji informatycznych lub sieci;
- przypadkowe bądź celowe modyfikowanie systemów i aplikacji informatycznych lub sieci;
- przypadkowe bądź celowe wprowadzenie zmian do chronionych danych osobowych;
- brak rejestrowania zdarzeń tworzenia lub modyfikowania danych.

4. W systemie informatycznym Szkoły przetwarzane są dane osobowe pracowników i uczniów Szkoły.

IV. ZASADY INFORMATYCZNEGO REJESTROWANIA I WYREJESTROWANIA UŻYTKOWNIKÓW SYSTEMU, ZAKRES ODPOWIEDZIALNOŚCI ADMINISTRATORA SYSTEMU

1. Rejestracji i wyrejestrowania użytkownika systemu informatycznego dokonuje upoważniona przez Administratora Danych Osobowych osoba ujęta w ewidencji osób uprawnionych do przetwarzania danych osobowych zwana Administratorem Bezpieczeństwa Informacji.
2. Każdy użytkownik upoważniony do pracy w systemie informatycznym, w którym przetwarzane są dane osobowe, winien posiadać własny odrębny identyfikator i hasło dostępu.
3. Rozwiązanie stosunku pracy, bądź zmiana zakresu obowiązków powoduje utratę

dostępu do przetwarzania danych i natychmiastowe wyrejestrowanie użytkownika z systemu oraz wykreślenie z ewidencji.

V. ZASADY DOPUSZCZANIA PRACOWNIKÓW DO EKSPLOATACJI SYSTEMÓW INFORMATYCZNYCH PRZETWARZAJĄCYCH ZBIORY DANYCH OSOBOWYCH

Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do zbierania lub przetwarzania danych osobowych, mogą być dopuszczeni wyłącznie pracownicy posiadający aktualne, ważne upoważnienia.

Administrator Bezpieczeństwa Informacji zapoznaje pracowników z przepisami o ochronie danych osobowych oraz wykazem akt i wiadomości stanowiących tajemnicę służbową (w zakresie ochrony danych osobowych).

VI. ZASADY TWORZENIA I POSŁUGIWANIA SIĘ HASŁAMI DOSTĘPU DO SYSTEMÓW INFORMATYCZNYCH

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym użytkownik może mieć wyłącznie po podaniu nazwy użytkownika (loginu) oraz właściwego hasła.
2. Należy wybierać hasła, które:
   - nie są hasłami słownikowymi,
   - składają się z co najmniej ośmiu znaków,
   - zawierają zarówno duże jak i małe litery oraz cyfry.
3. Hasło nie może być zapisywane lub przechowywane w miejscu dostępnym dla osób nieuprawnionych.
4. Okres ważności hasła ustawiony jest na okres nie dłuższy niż 1 miesiąc.
5. W przypadku utracenia hasła użytkownik ma obowiązek skontaktować się z ABI celem uzyskania nowego hasła.
6. Użytkownicy nie mogą korzystać z innych loginów (nazw użytkownika) niż te, do których są upoważnieni.
7. Szczególnej ochronie podlega hasło Administratora Bezpieczeństwa Informacji.

VII. PROCEDURY ROZPOCZĘCIA, KONTYNUOWANIA I ZAKOŃCZENIA PRACY Z SYSTEMEM INFORMATYCZNYM

1. Użytkownik rozpoczynający pracę zobowiązany jest do sprawdzenia zabezpieczenia pomieszczenia, w którym przetwarzane są dane osobowe, swojego stanowiska pracy oraz stanu sprzętu komputerowego, na którym pracuje.

2. Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy, każdy pracownik jest obowiązany do zwrócenia bacznej uwagi, czy nie wystąpiły objawy, mogące świadczyć o naruszeniu zasad ochrony danych osobowych. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje uruchomienie komputera, wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.
3. Krótkotrwałe przerwy w pracy (bez opuszczania stanowiska pracy) nie wymagają zamykania aplikacji.
4. Odchodząc od swojego komputera, każdy użytkownik powinien aktywować wygaszacz ekranu zabezpieczony hasłem dostępu lub zablokować dostęp do komputera naciskając klawisz z logo Windows i klawisz L.
5. Przed całkowitym opuszczeniem stanowiska pracy, użytkownik obowiązany jest zamknąć aplikację i wylogować się z pracy w sieci.
6. Zakończenie pracy polega na zamknięciu wszystkich programów i zapisaniu wszystkich otwartych plików oraz wybraniu odpowiedniego polecenia systemowego umożliwiającego zakończenie pracy. Użytkownik powinien zaczekać przy komputerze do chwili jego wyłączenia.
7. Pomieszczenia, w których przetwarzane są dane osobowe po zakończeniu pracy zamyka się na klucz.

VIII. PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH OSOBOWYCH ORAZ PROGRAMÓW I URZĄDZEŃ PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

A. ZASADY TWORZENIA KOPII ZAPASOWYCH

1. Na koniec każdego miesiąca Administrator Bezpieczeństwa Informacji na dyskach magnetycznych tworzy kopie zapasowe wszystkich zbiorów danych oraz programów i narzędzi programowych, w których przetwarzane są dane osobowe. Procedura tworzenia kopii zapasowych obejmuje wszystkie komputery, na których przetwarzane są dane osobowe.
2. Nośnik z nagranymi kopiami zapasowymi jest umieszczany w szafie zamykanej na klucz.
3. W każdym miesiącu dokonywany jest przegląd przechowywanych nośników kopii zapasowych, w celu usunięcia zbędnych danych. Nieprzydatne już nośniki informacji pozbawia się w sposób trwały zapisanych danych osobowych.
4. Dodatkowo należy sporządzać kopie roczne, bilansowe.

B. ZASADY PRZECHOWYWANIA NOŚNIKÓW INFORMACJI ZE ZBIORAMI DANYCH (W TYM DANYCH OSOBOWYCH) ORAZ KOPII BEZPIECZEŃSTWA

1. Nośniki elektroniczne przeznaczone do przechowywania danych osobowych powinny się charakteryzować odpowiednią trwałością zapisu, zależną od planowanego okresu przechowywania na nich danych.
2. Nośniki informatyczne zawierające dane osobowe oraz kopie zapasowe zbiorów danych osobowych, programów i narzędzi programowych służących do przetwarzania danych osobowych, przechowywane są w szafie zamykanej na klucz w sekretariacie Szkoły. Dostęp do nośników o których mowa ograniczony jest do Administratora Bezpieczeństwa Informacji oraz upoważnionego przez niego pracownika.
3. Czas przechowywania kopii zapasowych zbiorów lokalnych ustala się na:
   - kopia codzienna (jeżeli wymagana) - 1 tydzień
   - kopia tygodniowa (piątkowa - jeżeli wymagana) - 1 miesiąc
   - kopia miesięczna - 1 rok
   - kopia roczna (ostatni dzień okresu bilansowego) - 5 lat
4. Miejsca przechowywania kopii bezpieczeństwa muszą podlegać szczególnej ochronie.

IX. ZASADY NISZCZENIA ISPOSOBY DOKUMENTOWANIA PROCESU NISZCZENIA NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE

1. Jeżeli usunięcie danych osobowych z nośników magnetycznych nie jest możliwe wówczas nośniki zostają uszkodzone w sposób uniemożliwiający ich odczytanie.
2. Nośniki papierowe (wydruki) nie przeznaczone do ponownego użytku oraz nie archiwizowane powinny być natychmiast niszczone.

X. OKREŚLENIE ZASAD ZABEZPIECZANIA ORAZ WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

1. Z uwagi na fakt, iż niektóre wykorzystywane komputery przetwarzające dane osobowe posiadają dostęp do sieci publicznej, Administrator Bezpieczeństwa Informacji powinien wdrożyć procedury oraz oprogramowanie, które chroni dane osobowe przed nieuprawnionym dostępem, zmianami, usunięciem lub uszkodzeniem. Zagrożenia te to programy zawierające złośliwy kod (wirusy), tzw. konie trojańskie oraz ataki hakerów.

2. We wszystkich komputerach zainstalowanych w Szkole może być instalowane wyłącznie legalne oprogramowanie posiadające licencję, certyfikat legalności itp.
3. Zabronione jest pobieranie oraz instalowanie bez nadzoru osoby upoważnionej przez Administratora Bezpieczeństwa Informacji, jakichkolwiek programów na komputerach służących do przetwarzania danych osobowych.
4. Zabronione jest używanie nośników informacji nie pochodzących z zasobów Administratora Bezpieczeństwa Informacji.
5. Każda osoba przetwarzająca dane osobowe przy użyciu komputera musi być pouczona, aby w wypadku jakichkolwiek podejrzeń dotyczących obniżenia bezpieczeństwa danych osobowych, poinformowała o tym fakcie osobę upoważnioną przez Administratora Danych Osobowych, samego Administratora Danych Osobowych lub Administratora Bezpieczeństwa Informacji.
6. Za legalność użytkowanego oprogramowania specjalistycznego odpowiada użytkownik systemu.

Do usuwania wirusów należy używać programów antywirusowych, pozostających w dyspozycji jednostki.

XI. ZABEZPIECZENIE PRZED DZIAŁANIEM OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

Dla potrzeb systemu informatycznego w Szkole stosowane jest zabezpieczenie antywirusowe:

- Ochrona poczty:NOD 32 ESET ENDPOINT ANTIVIRUS.
- Ochrona przeglądanych stron: NOD 32 ESET ENDPOINT ANTIVIRUS.
- Ochrona systemów plików: NOD 32 ESET ENDPOINT ANTIVIRUS.
- Sieć szkolna zabezpieczona przez router z firewall-em i NAT.
- Oprogramowanie Opiekun ucznia – chroniący przed wejściem na niepowołane, niewłaściwe strony.
- Kontrola komputerów w oparciu o Active Directory (dostęp do danych, urządzeń zewnętrznych.

XII. POSTĘPOWANIE W ZAKRESIE KOMUNIKACJI SIECIOWEJ

1. Przeglądarka (jeżeli jest to możliwe) powinna mieć ustawione opcje tak, by nie zapamiętywała nazwy użytkownika oraz hasła.
2. Komunikacja w sieci komputerowej dozwolona jest tylko po odpowiednim zalogowaniu się i podaniu indywidualnego hasła użytkownika.

3. Dostęp do wszystkich folderów i plików z sieci zabezpieczony jest odpowiednimi uprawnieniami.

XIII. POSTANOWIENIA KOŃCOWE

1. Każda osoba wpisana do ewidencji zobowiązana jest do odbycia stosownego przeszkolenia w zakresie ochrony danych osobowych oraz zapoznania się z:
   - treścią ustawy oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzaniadanych osobowych oraz warunków technicznychi organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
   - polityką bezpieczeństwa –regulaminem ochrony danych osobowych;
   - instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
   - uregulowaniami wewnętrznymi obowiązującymi w tym zakresie.
2. Wykonanie powyższych zobowiązań pracownik potwierdza własnoręcznym podpisem.
3. Wszelkie zagadnienia dotyczące ochrony danych osobowych nie ujęte w niniejszej „Instrukcji" należy rozpatrywać zgodnie z treścią aktów prawnych wymienionych w regulaminie ochrony danych osobowych, z uwzględnieniem późniejszych zmian i uzupełnień.
4. Instrukcja niniejsza wchodzi w życie z dniem zatwierdzenia jej przez Dyrektora Szkoły (Administratora Danych Osobowych).