Noworudzka Szkoła Techniczna

w Nowej Rudzie

57-401 Nowa Ruda, ul. Stara Droga 4, tel. 074 872 22 42, fax 074 872 94 14, e-mail: szkola@zsp.nowaruda.pl

POLITYKA BEZPIECZEŃSTWA

W ZAKRESIE OCHRONY DANYCH OSOBOWYCH

NOWA RUDA, WRZESIEŃ 2013

I. POSTANOWIENIA OGÓLNE

§ 1

Polityka bezpieczeństwa przetwarzania danych osobowych Noworudzkiej Szkole Technicznej w Nowej Rudzie zwana dalej „Polityką bezpieczeństwa", określa podstawowe zasady dotyczące zapewnienia bezpieczeństwa w zakresie danych osobowych przetwarzanych w zbiorach danych:

1) tradycyjnych, w szczególności kartotekach, księgach, skorowidzach, aktach osobowych, wykazach, w zbiorach ewidencyjnych;

2) w systemach informatycznych, w szczególności deklaracje ZUS, ewidencje płacowe, stypendialne, informacje skarbowe, ewidencje statystyczne, plany organizacyjne.

§ 2

1. Dane osobowe w Noworudzkiej Szkole Technicznej w Nowej Rudzie przetwarzane są z poszanowaniem obowiązujących w tym zakresie przepisów prawa, a w szczególności:

   1) przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity z 2002 r.: Dz.U.Nr101,poz.926 z późniejszymi zmianami) oraz przepisów wykonawczych z nią związanych,

   2) przepisów art.221 §1 - 5 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jednolity z 1998 r.: Dz.U.Nr21, poz.94 z późniejszymi zmianami) i przepisów wykonawczych z nią związanych,

   3) Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku, 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. Nr 100, póz. 1024)

   4) oraz innych przepisów ustaw i rozporządzeń normujących przetwarzanie danych osobowych określonych kategorii.

2. Dane osobowe w Noworudzkiej Szkole Technicznej w Nowej Rudzie przetwarzane są w celu realizacji statutowych celów Szkoły. W szczególności dane osobowe przetwarza się:

   1) dla zabezpieczania prawidłowego toku realizacji zadań dydaktycznych, organizacyjnych Szkoły

   2) w celu zapewnienia prawidłowej, zgodnej z prawem i celami Szkoły polityki personalnej

   3) oraz bieżącej obsługi stosunków pracy, a także innych stosunków zatrudnienia nawiązywanych przez Szkołę działająca jako pracodawca w rozumieniu art. 3 kodeksu pracy lub strona innych stosunków zatrudnienia.

   1) dla realizacji innych usprawiedliwionych celów i zadań Szkoły - z poszanowaniem praw i wolności osób powierzających swoje dane.

§ 3

1. Każdy z pracowników Noworudzkiej Szkole Technicznej w Nowej Rudzie ma prawo do ochrony dotyczących go danych osobowych.
2. Przetwarzanie danych osobowych może mieć miejsce ze względu na dobro publiczne, dobro osoby, której dane dotyczą, lub dobro osób trzecich w zakresie i trybie określonym regulaminem.

3. Za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

§ 4

Ilekroć w regulaminie jest mowa o:

1) zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

2) 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.

II OSOBY PRZETWARZAJACE DANE OSOBOWE

§ 5

1) Administratorem Danych osobowych w Noworudzkiej Szkole Technicznej w Nowej Rudzie jest Dyrektor Szkoły.

2) Administrator Danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były:

   - przetwarzane zgodnie z prawem,
   - zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami
   - merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
   - przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

3) Przetwarzanie danych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą.

4) Administrator Danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 6

1) Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych.
2) Administrator Danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.
3) Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.

§ 7

1) Administrator Danych może upoważnić pracowników szkoły: pedagogicznych i niepedagogicznych lub na ich wniosek udzielić upoważnienia do przetwarzania danych osobowych w Noworudzkiej Szkole Technicznej w Nowej Rudzie
2) Upoważnienia, o których mowa w ust. 1, są imienne i udzielane w formie pisemnej na czas określony lub na czas nieokreślony – do odwołania udzielonego upoważnienia.
3) Wniosek, o którym mowa w ust. 1, winien precyzyjnie określać zakres spraw objętych upoważnieniem.
4) Każde upoważnienie jest rejestrowane w rejestrze upoważnień oraz przechowywane w aktach osobowych pracownika.

§ 8

Osoby, które zostały upoważnione do przetwarzania danych zobowiązane są do:

1. Zachowania szczególnej staranności przy gromadzeniu danych, aby dane te były:
    a. przetwarzane zgodnie z prawem,
    b. zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu, przetwarzaniu niezgodnemu z tymi celami.
    c. merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
2. Poprawnego korzystania z aplikacji zgodnie z powierzonymi obowiązkami służbowymi
3. Informowanie Administratora Systemu o wszelkich nieprawidłowościach działania Aplikacji,
4. Ustalenie hasła, okresowe zmiany haseł,
5. Utrzymywanie w ścisłej tajemnicy haseł, którymi się posługuje

6. Zmianę hasła w przypadku powzięcia przez użytkownika podejrzenia lub stwierdzenia, że z hasłem mogły zapoznać się osoby trzecie i powiadomienie o tym fakcie Administratora Bezpieczeństwa Informacji
7. Zgłaszanie awarii urządzeń komputerowych, oprogramowania systemowego, sieci komputerowej administratorowi systemu.

§ 9

Administrator Danych powołuje Administratora Bezpieczeństwa Informacji odpowiedzialnego jest za:

1. Realizację ustawy o ochronie danych osobowych w zakresie dotyczącym Administratora
1. Bezpieczeństwo informacji,
2. Zapewnienie, że do informacji chronionych mają dostęp wyłącznie osoby upoważnione, oraz że mogą one wykonywać wyłącznie uprawnione operacje,
3. Zabezpieczenie obszarów przetwarzania danych osobowych w sposób uniemożliwiający dostęp do nich osób trzecich,
4. Ewidencjonowanie udostępniania danych zgodnie z ustawą o ochronie danych osobowych,
5. Weryfikację dopuszczenia użytkowników do przetwarzania danych,
6. Powiadomienie Administratora Systemu o konieczności utworzenia identyfikatora użytkownika w systemie,
7. Powiadomienie Administratora Systemu o zmianie uprawnień dostępu użytkownika do systemu

§ 10

Administrator Danych powołuje Administratora Systemu informacji, który odpowiedzialny jest za:

1. Bieżący monitoring oraz zapewnianie ciągłości działania systemu informatycznego,
2. Optymalizacja wydajności systemu informatycznego,
3. Instalacje i konfiguracje sprzętu sieciowego i serwerowego,
4. Instalacje i konfiguracje oprogramowania systemowego i sieciowego,
5. Konfigurację i administrację oprogramowaniem systemowym i sieciowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,
6. Współpracę z dostawcami usług i sprzętu sieciowego, serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,
7. Zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego i sieciowego,

8. Zarządzanie kopiami awaryjnymi danych w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie,

9. Przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,

10. Udostępnianie danych zgromadzonych w Systemie Informatycznym, na wniosek Administratora Danych (w rozumieniu ustawy o ochronie danych osobowych) za zgodą Administratora Bezpieczeństwa Informacji,

11. Prowadzenie zakupów urządzeń sieciowych i serwerowych,

12. Prowadzenie zakupów oprogramowania sieciowego i serwerowego,

13. Wnioskowanie do Administratora Bezpieczeństwa Informacji w sprawie procedurach bezpieczeństwa i standardów zabezpieczeń.

III. PRAWA OSÓB , KTÓRYCH DANE SA PRZETWARZANE PRZEZ NOWORUDZKĄ SZKOŁĘ TECHNICZNĄ

Art. 11

1. Szkoła gwarantuje osobom fizycznym, których dane osobowe są przetwarzane w związku z realizacją jego celów statutowych, realizacje uprawnień gwarantowanych im przez obowiązujące przepisy prawa.
2. W szczególności każdej osobie fizycznej, której dane osobowe są przetwarzane w związku z realizacja celów statutowych Szkoły, przysługuje prawo do uzyskania informacji o zakresie jej uprawnień związanych z ochroną danych osobowych, a także prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych na zasadach określonych w art. 32 – 35 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
3. Osoby fizyczne, których dane osobowe są przetwarzane w związku z realizacja celów statutowych Szkoły, uzyskują informacje o przysługujących im prawach w sposób przyjęty w poszczególnych jednostkach organizacyjnych Noworudzkiej Szkole Technicznej w Nowej Rudzie

IV. ZBIORY DANYCH OSOBOWYCH TWORZONE W NOWORUDZKIEJ SZKOLE TECHNICZNEJ W NOWEJ RUDZIE

Noworudzka Szkoła Techniczna w Nowej Rudzie realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych zabrania tworzenia zbiorów danych osobowych, a także gromadzenia w zbiorach lub poza nimi kategorii danych osobowych innych niż niezbędne dla realizacji celów statutowych Szkoły.

§ 13

Wykaz zbiorów danych osobowych stanowi załącznik niniejszego regulaminu.

V. POSTANOWIENIA KOŃCOWE

§ 14

Postanowienia niniejszego regulaminu stosuje odpowiednio do przetwarzania danych osobowych w systemach informatycznych , listach płac, księgach uczniów, kartotekach, wykazach , rejestrach , zaświadczeniach, archiwum i innych zbiorach ewidencyjnych.

§ 15

Regulamin wchodzi w życie z dniem ogłoszenia i wymaga dla swej ważności pisemnego oświadczenia wszystkich użytkowników o zapoznaniu się z jego postanowieniami.

Spis załączników:

1) Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych w Noworudzka Szkoła Techniczna w Nowej Rudzie jest określony w załączniku nr 1 do regulaminu.

2) Wzór imiennego upoważnienia do przetwarzania danych osobowych w NST obejmujących następujący zakres: dane osobowe uczniów/słuchaczy, rodziców/opiekunów prawnych, niezbędnych do prowadzenia dokumentacji szkolnej oraz dla celów egzaminów jest określony w załączniku nr 2 do regulaminu.

3) Wzór imiennego upoważnienia do przetwarzania danych osobowych pracowników, w zakresie dotyczącym przetwarzania danych zgodnie z zakresem obowiązków i uprawnień jest określony w załączniku nr 3 do regulaminu.

4) Wzór wniosku o udzielenie upoważnienia do przetwarzania danych osobowych jest określony w załączniku nr 4 do regulaminu.

5) Wykaz zbiorów danych osobowych – załącznik nr 5

6) Wzór zarządzenia w sprawie powołania Administratora Bezpieczeństwa Informacji zał. nr 6

7) Wzór zaświadczenia o odbytym przeszkoleniu w zakresie ochrony danych osobowych – zał. nr 7

8) Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych zał. nr 8

Nowa Ruda, 25 września 2013 roku

Załącznik nr 1 do Regulaminu „Polityka
bezpieczeństwa w zakresie ochrony danych osobowych”
w Noworudzkiej Szkole Technicznej

WZÓR
Ewidencji osób upoważnionych do przetwarzaniu danych osobowych
w Noworudzkiej Szkole Technicznej w Nowej Rudzie

L.p.	Imię i nazwisko	Data nadania	Data ustania	Zakres upoważnienia	Podpis

Załącznik nr 2 do Regulaminu „Polityka bezpieczeństwa w zakresie ochrony danych osobowych" w Noworudzkiej Szkole Technicznej w Nowej Rudzie

WZÓR UPOWAŻNIENIA

…… Nowa Ruda ……..
Pieczątka szkoły *data wydania*

Upoważnienie nr …….

Upoważniam Pana/Panią …….. do przetwarzania danych osobowych w NST w Nowej Rudzie obejmujących następujący zakres: **dane osobowe uczniów/słuchaczy, rodziców/ opiekunów prawnych, niezbędnych do prowadzenia dokumentacji szkolnej oraz dla celów egzaminów.**

Równocześnie zobowiązuję Pana/Panią …… do zachowania w tajemnicy wszelkich informacji dotyczących przetwarzania danych osobowych oraz sposobu ich zabezpieczenia.

Informuję, że udostępnianie danych osobowych lub umożliwianie dostępu do nich osobie nieuprawnionej podlega karze grzywnej, karze ograniczenia wolności do lat dwóch.

Podstawa prawna: art. 51 ustawy z dnia z dnia 29 sierpnia 1997r. o ochronie danych osobowych (t.j. Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.)

Upoważnienie jest ważne od dnia …….. do dnia ……

do dnia …….. do odwołania.

…….. ……..

data i podpis upoważnionego *data i podpis administratora danych*

Załącznik nr 3 do Regulaminu „Polityka bezpieczeństwa w zakresie ochrony danych osobowych" w Noworudzkiej Szkole Technicznej w Nowej Rudzie

……, dnia ……

Upoważnienie

do przetwarzania danych osobowych

Na podstawie art. 37 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) upoważniam Panią / Pana:

.....

(imię i nazwisko osoby upoważnionej)

zatrudnioną (ego) w

.....

(nazwa jednostki i komórki organizacyjnej)

na stanowisku:

.....

do przetwarzania od dnia ..... danych osobowych w zakresie :

Numer/nazwa zbioru	**zakres**
Zbiór nr 1 – Księga druków ścisłego zarachowania	
Zbiór nr 2 – Akta osobowe pracowników	
Zbiór nr 3 – Ewidencja zwolnień lekarskich pracowników	
Zbiór nr 4 – Księga zastępstw nauczycieli – rejestr elektroniczny „Zastępstwa"	
Zbiór nr 5 – Protokoły Rady Pedagogicznej	
Zbiór nr 6 – Ewidencja urlopów pracowników niepedagogicznych	
Zbiór nr 7 – Ewidencja osób korzystających z księgozbioru bibliotecznego	
Zbiór nr 8 – Ewidencja legitymacji pracowniczych	
Zbiór nr 9 – Ewidencja legitymacji ubezpieczeniowych	
Zbiór nr 10 – Rejestr delegacji służbowych	
Zbiór nr 11 – Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych	
Zbiór nr 12 – Ewidencja osób korzystających ze świadczeń Funduszu Socjalnego	
Zbiór nr 13 – Listy płac pracowników – rejestr elektroniczny „Płace"	
Zbiór nr 14 – Księga ewidencji uczniów – rejestr elektroniczny „Sekretariat"	

Zbiór nr 15 – Dzienniki lekcyjne i pozalekcyjne – dziennik elektroniczny „Librus”	
Zbiór nr 16 – Rejestr pedagoga szkolnego	
Zbiór nr 17 – Arkusze ocen wszystkich uczniów wraz z opiniami poradni PPP – rejestr elektroniczny „Sekretariat”	
Zbiór nr 18 – Protokoły egzaminów klasyfikacyjnych i poprawkowych	
Zbiór nr 19 – Ewidencja wydanych legitymacji szkolnych – rejestr elektroniczny „Sekretariat”	
Zbiór nr 20 – Ewidencja wydanych świadectw ukończenia szkoły	
Zbiór nr 21 – Rejestr wypadków uczniów	
Zbiór nr 22 – Archiwum (akta osobowe pracowników, listy płac, księgi arkuszy ocen, dzienniki lekcyjne)	
Zbiór nr 23 – Arkusz organizacji roku szkolnego – rejestr elektroniczny „Arkusz organizacyjny”	
Zbiór nr 24 – Akta osobowe pracowników – rejestr elektroniczny „Kadry”	

.....

(Administrator Danych)

Załącznik nr 4 do Regulaminu „Polityka bezpieczeństwa w zakresie ochrony danych osobowych" w Noworudzkiej Szkole Technicznej w Nowej Rudzie

WZÓR WNIOSKU

…… Nowa Ruda ……..
Imię i nazwisko wnioskodawcy *data*

……..
Stanowisko

Wniosek

Proszę o udzielenie upoważnienia do dostępu do danych osobowych
……
…….. w zakresie dotyczącym przetwarzania danych w celu
……
……

Jednocześnie zobowiązuję się do zachowania w tajemnicy informacji, z którymi zapoznam się podczas korzystania z
……
……

Proszę o udzielenie upoważnienia w okresie …….. ,

od dnia …….. do dnia ……..

……..

data i podpis wnioskodawcy

ZBIORY DANYCH OSOBOWYCH W ZSP Nowa Ruda

Dane osobowe są gromadzone, przechowywane i przetwarzane w kartotekach, skorowidzach, księgach, wykazach oraz w innych zbiorach ewidencyjnych poszczególnych komórek organizacyjnych Jednostki w postaci dokumentów papierowych.

Do przetwarzania zbiorów danych osobowych w systemie informatycznym Jednostki, stosowane są pakiety biurowe lub specjalizowane programy:

W szkole tworzy się następujące zbiory danych osobowych:

Zbiór nr 1 – Księga druków ścisłego zarachowania

Zbiór nr 2 – Akta osobowe pracowników

Zbiór nr 3 – Ewidencja zwolnień lekarskich pracowników

Zbiór nr 4 – Księga zastępstw nauczycieli – rejestr elektroniczny „Zastępstwa"

Zbiór nr 5 – Protokoły Rady Pedagogicznej

Zbiór nr 6 – Ewidencja urlopów pracowników niepedagogicznych

Zbiór nr 7 – Ewidencja osób korzystających z księgozbioru bibliotecznego

Zbiór nr 8 – Ewidencja legitymacji pracowniczych

Zbiór nr 9 – Ewidencja legitymacji ubezpieczeniowych

Zbiór nr 10 – Rejestr delegacji służbowych

Zbiór nr 11 – Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych

Zbiór nr 12 – Ewidencja osób korzystających ze świadczeń Funduszu Socjalnego

Zbiór nr 13 – Listy płac pracowników – rejestr elektroniczny „Płace"

Zbiór nr 14 – Księga ewidencji uczniów – rejestr elektroniczny „Sekretariat"

Zbiór nr 15 – Dzienniki lekcyjne i pozalekcyjne – dziennik elektroniczny „Librus"

Zbiór nr 16 – Rejestr pedagoga szkolnego

Zbiór nr 17 – Arkusze ocen wszystkich uczniów wraz z opiniami poradni PPP – rejestr elektroniczny „Sekretariat"

Zbiór nr 18 – Protokoły egzaminów klasyfikacyjnych i poprawkowych

Zbiór nr 19 – Ewidencja wydanych legitymacji szkolnych – rejestr elektroniczny „Sekretariat"

Zbiór nr 20 – Ewidencja wydanych świadectw ukończenia szkoły

Zbiór nr 21 – Rejestr wypadków uczniów

Zbiór nr 22 – Archiwum (akta osobowe pracowników, listy płac, księgi arkuszy ocen, dzienniki lekcyjne)

Zbiór nr 23 – Arkusz organizacji roku szkolnego – rejestr elektroniczny „Arkusz organizacyjny"

Zbiór nr 24 – Akta osobowe pracowników – rejestr elektroniczny „Kadry"

Załącznik nr 6 do Regulaminu „Polityka bezpieczeństwa w zakresie ochrony danych osobowych" w Noworudzkiej Szkole Technicznej w Nowej Rudzie

ZARZĄDZENIE Nr.....

Dyrektor Noworudzkiej Szkoły Technicznej w Nowej Rudzie

z dnia.....

w sprawie powołania Administratora Bezpieczeństwa Informacji

Na podstawie art.36 ust.3 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz Regulaminu „**POLITYKA BEZPIECZEŃSTWA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH**

u s t a n a w i a m

z dniem ……

Pana/Panią……

…….

ADMINISTRATOREM BEZPIECZEŃSTWA INFORMACJI

w Noworudzkiej Szkole Technicznej w Nowej Rudzie

Zakres czynności dla Administratora Bezpieczeństwa Informacji stanowi załącznik do niniejszego zarządzenia.

Załącznik do Zarządzenia Nr……z dnia.....

Zakres czynności Administratora Bezpieczeństwa Informacji w *Noworudzkiej Szkole Technicznej* w Nowej Rudzie

1. Przeciwdziałanie dostępowi osób niepowołanych do systemu , w którym przetwarzane są dane osobowe,
2. Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń zabezpieczeń lub podejrzenia naruszenia w systemie ,
3. Nadzór nad fizycznym zabezpieczeniem pomieszczeń , w których przetwarzane są dane osobowe oraz nadzór nad kontrolą przebywających w nich osób,
4. Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych na których zapisane są dane osobowe,
5. Zarządzanie hasłami użytkowników, systemami antywirusowymi i ich procedurami,
6. Nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności,
7. Nadzór nad obiegiem dokumentów zawierających dane osobowe,
8. Nadzór nad prawidłowością archiwizacji oraz usuwania danych osobowych,
9. Monitorowanie funkcjonowania zabezpieczeń wdrożonych celu ochrony danych osobowych,
10. Nadzór nad prowadzeniem wymaganej dokumentacji,
11. Wdrożenie szkoleń z zakresu przepisów dotyczących ochrony danych oraz stosowania środków technicznych i organizacyjnych przy przetwarzaniu danych w systemach informatycznych.

Załącznik nr 7 do Regulaminu „Polityka bezpieczeństwa w zakresie ochrony danych osobowych" w Noworudzkiej Szkole Technicznej w Nowej Rudzie

……

/ nazwa jednostki organizacyjnej/

ZAŚWIADCZENIE Nr……

stwierdzające odbycie przeszkolenia w zakresie ochrony danych osobowych

Stwierdza się, że Pan/i/:

- imię i nazwisko :……

- data urodzenia:……

odbył/a/ w ……

przeszkolenie w zakresie ochrony danych osobowych wymagane przepisami ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 roku (t.j Dz.U.

z 2002 r., poz.1204, z późn.zm.)

…… **……**

/miejscowość i data/ /administrator bezpieczeństwa /

Załącznik nr 8 do Regulaminu „Polityka bezpieczeństwa w zakresie ochrony danych osobowych" w Noworudzkiej Szkole Technicznej w Nowej Rudzie

Załącznik do zarządzenia Nr……. z dnia……..

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

w Noworudzkiej Szkole Technicznej w Nowej Rudzie

Opracował : ……

/ imię i nazwisko /

Administrator Bezpieczeństwa Informacji

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych *w Noworudzkiej Szkole Technicznej* w Nowej Rudzie Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę Szkoły. Dokument zwraca uwagę na konsekwencje jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

1. Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym.
2. Instrukcja określa tryb postępowania w przypadku, gdy:
    1) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
    2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.
3. Instrukcja obowiązuje wszystkich pracowników Noworudzkiej Szkole Technicznej w Nowej Rudzie
4. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznych

Rozdział 1

OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

1. Podział zagrożeń:

1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
3) zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie

naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są

dane osobowe to głównie:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,

3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
6) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.,
12) podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,
13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej itp.

Rozdział 2

ZABEZPIECZENIE DANYCH OSOBOWYCH

1. Administratorem Danych osobowych zawartych i przetwarzanych w systemach informatycznych Szkoły jest Dyrektor.
2. Administrator Danych osobowych jest obowiązany do zastosowania środków
    1. technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych jednostki, a w szczególności:
        a. zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
        b. zapobiegać przed zabraniem danych przez osobę nieuprawnioną,
        c. zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.
    2. Do zastosowanych środków technicznych należy:
        a. przetwarzanie danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej,
        b. zabezpieczenie wejścia do pomieszczeń, o których mowa w pkt. 1,
        c. szczególne zabezpieczenie centrum przetwarzania danych (komputer centralny serwerownia) poprzez zastosowanie systemu kontroli dostępu,
        d. wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji,

3. Do zastosowanych środków organizacyjnych należą przede wszystkim następujące zasady:
    1. zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych,
    2. przeszkolenie osób, o których mowa w pkt. 1, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych,
    3. kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę.
4. Niezależnie od niniejszych zasad opisanych Instrukcji w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie.

Rozdział 3

KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Administrator danych lub osoba przez niego wyznaczona, którą jest „Administrator Bezpieczeństwa Informacji" sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.

Rozdział 4

POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. W przypadku stwierdzenia naruszenia:
    a. zabezpieczenia systemu informatycznego,
    b. technicznego stanu urządzeń,
    c. zawartości zbioru danych osobowych,
    d. ujawnienia metody pracy lub sposobu działania programu,
2. jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
3. innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.)

<u>każda osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa.</u>

4. W razie niemożliwości zawiadomienia Administratora Bezpieczeństwa lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego,
5. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora

Bezpieczeństwa lub upoważnionej przez niego osoby, należy:

- niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
- rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
- zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
- podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
- podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
- zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
- udokumentować wstępnie zaistniałe naruszenie,
- nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa lub osoby upoważnionej.

6. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Bezpieczeństwa lub osoba go zastępująca:
   - zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy jednostki,
   - może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
   - rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora Danych ,
   - nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Jednostki.
7. Administrator Bezpieczeństwa dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego załącznik, który powinien zawierać w szczególności:
   - wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
   - określenie czasu i miejsca naruszenia i powiadomienia,
   - określenie okoliczności towarzyszących i rodzaju naruszenia,
   - wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
   - wstępną ocenę przyczyn wystąpienia naruszenia,
   - ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.
8. Raport, o którym mowa w ust. 7, Administrator Bezpieczeństwa niezwłocznie przekazuje Administratorowi Danych (kierownikowi jednostki), a w przypadku jego nieobecności osobie uprawnionej.

9. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator Bezpieczeństwa zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.
10. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Kierownictwo Jednostki, Administratora Bezpieczeństwa Informacji,
11. Analiza, o której mowa w ust. 10, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Rozdział 5

MONITOROWANIE ZABEZPIECZEŃ

1. Prawo do monitorowania systemu zabezpieczeń posiadają , zgodnie z zakresem czynności:
   a) Administrator Danych,
   b) Administrator Bezpieczeństwa Informacji.
2. W ramach kontroli należy zwracać szczególna uwagę na:
   a) okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do możliwości odtwarzania danych,
   b) kontrola ewidencji nośników magnetycznych,
   c) kontrola właściwej częstotliwości zmiany haseł .

Rozdział 6

SZKOLENIA

1. Wszyscy pracownicy Jednostki mają obowiązek brać udział w szkoleniach ,
2. Szkolenie powinno dotyczyć:
   a) obowiązujących przepisów i instrukcji wewnętrznych dotyczących ochrony danych osobowych, sposobu niszczenia wydruków i zapisów na nośnikach magnetycznych i optycznych,
   b) przedstawienie zasad ochrony danych osobowych dotyczących bezpośrednio wykonywanych obowiązków na stanowisku pracy.

Rozdział 7

NISZCZENIE WYDRUKÓW I ZAPISÓW NA NOŚNIKACH MAGNETYCZNYCH

NOŚNIKI MAGNETYCZNE PRZEKAZYWANE NA ZEWNĄTRZ POWINNY BYĆ POZBAWIONE ZAPISÓW ZAWIERAJĄCYCH DANE OSOBOWE.,

1. Niszczenie poprzednich zapisów powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika,
2. Poprawność przygotowania nośnika magnetycznego powinna być sprawdzona przez Administratora Bezpieczeństwa Informacji,
3. Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć poprzez przecięcie, przełamanie itp.
4. Wydruki po wykorzystaniu należy zniszczyć w mechanicznej niszczarce do papieru.

Rozdział 8

ARCHIWIZACJA DANYCH

1) Dane systemów kopiowane są w systemie tygodniowym,
2) Kopie awaryjne danych zapisywanych w programach wykonywane są codziennie,

3) Odpowiedzialnym za wykonywanie kopii danych i kopii awaryjnych jest Administrator Bezpieczeństwa Informacji,
4) Na koniec danego miesiąca wykonywane są kopie bezpieczeństwa z całego programu przetwarzającego dane. Nośniki z kopiami bezpieczeństwa przechowywane są w (kasa Urzędu, kancelaria tajna itp.),
5) Kopie awaryjne przechowywane są w *(wyznaczonym pomieszczeniu lub instytucji , z którą podpisano stosowne porozumienie)*,
6) Dyskietki , na których zapisywane są kopie bezpieczeństwa są każdorazowo wymazywane i formatowane , w taki sposób , by nie można było odtworzyć ich zawartości.
7) Płyty CD , DVD na których przechowuje się kopie awaryjne niszczy się w sposób mechaniczny , tak by nie można było użyć ich ponownie,
8) Administrator Bezpieczeństwa Informacji odpowiedzialny jest za dokonywanie wymiany kopii awaryjnych na aktualne,
9) Administrator Bezpieczeństwa Informacji dokonuje okresowej weryfikacji kopii bezpieczeństwa pod kątem ich przydatności,

Rozdział 9

POSTANOWIENIA KOŃCOWE

1. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.

2. Administrator Bezpieczeństwa zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego załącznik do niniejszego dokumentu.

3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Administratora Bezpieczeństwa.

4. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia administratora bezpieczeństwa informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

5. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926), rozporządzenia 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. Nr 100, poz. 1024) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz. U. Nr 100, poz. 1023).