Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Zespół Szkół Samochodowych i Budowlanych
Im. Leonarda da Vinci
w Głogowie
ul. Piastowska 2a

SPIS TREŚCI

Wprowadzenie……..…..…3

Rozdział 1. Opis zdarzeń naruszających ochronę danych osobowych …..…….…….....4

Rozdział 2. Zabezpieczenie danych osobowych ……...…….……...5

Rozdział 3. Kontrola przestrzegania zasad zabezpieczenia danych osobowych ……....……..7

Rozdział 4. Postępowanie w przypadku naruszenia ochrony danych osobowych ……..…….8

Rozdział 5. Monitorowanie zabezpieczeń …….….....9

Rozdział 6. Szkolenia …….....10

Rozdział 7. Niszczenie wydruków i zapisów na nośnikach magnetycznych …….…….10

Rozdział 8. Archiwizacja danych …….....10

Rozdział 9. Postanowienia końcowe …….....11

Załącznik nr 1 – Wykaz pomieszczeń Zespołu Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie, w których przetwarza się dane osobowe, oraz osoby mające prawo wglądu do danych osobowych ……...13

Załącznik nr 2 – Raport z naruszenia bezpieczeństwa systemu informatycznego w Zespole Szkół Samochodowych i Budowlanych w Głogowie 14

Załącznik nr 3 – Wykaz osób, które zostały zapoznane z Polityką Bezpieczeństwa .....…...15

Załącznik nr 4 – Oświadczenie …...…….17

Załącznik nr 5 – Upoważnienie ...……18

Załącznik nr 6 – Zakres czynności pracownika zatrudnionego przy przetwarzaniu danych osobowych.……20

WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Zespole Szkół Samochodowych i Budowlanych im Leonarda da Vinci w Głogowie.

Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę Zespołu Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie . Dokument zwraca uwagę na konsekwencje jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym.

Dokument ,,**Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Zespole Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie",** zwany dalej ,,Polityką bezpieczeństwa", wskazujący sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych, przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych.

Potrzeba jego opracowania wynika z § 4 rozporządzenia Prezesa Rady Ministrów z dnia 25 sierpnia 2005 roku w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 171 poz. 1433) oraz § 3 i 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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).

1. ,,Polityka bezpieczeństwa" określa tryb postępowania w przypadku, gdy:
   a) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
   b) 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.
2. ,,Polityka bezpieczeństwa" obowiązuje wszystkich pracowników Zespołu Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie.
3. Wykonanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszania bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznych Zespołu Szkół Samochodowych i Budowlanych im. Leonarda da Vinci.
4. Administrator danych, którym jest Dyrektor Zespołu Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie, swoją decyzją wyznacza Administratora Bezpieczeństwa Informacji danych zawartych w systemach informatycznych Zespołu Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie, zwanego dalej ,,Administratorem Bezpieczeństwa".
5. ,,Administrator Bezpieczeństwa" realizuje zadnia w zakresie ochrony danych, a w szczególności:
   a) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Zespołu Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie,

b) podejmowania stosownych działań zgodnie z niniejszą ,,Polityką bezpieczeństwa" w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia bezpieczeństwa danych znajdujących się w systemie informatycznym,
c) niezwłocznego informowania Administratora danych lub osoby przez niego upoważnionej o przypadkach naruszania przepisów ustawy o ochronie danych osobowych,
d) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych,
e) osoba zastępująca Administratora Bezpieczeństwa powyższe zadania realizuje w przypadku nieobecności Administratora Bezpieczeństwa,
f) osoba zastępująca składa Administratorowi Bezpieczeństwa relację z podejmowanych działań w czasie jego zastępstwa.

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, nośnikach elektronicznych w formie niezabezpieczonej itp.

ROZDZIAŁ 2

ZABEZPIECZENIE DANYCH OSOBOWYCH

1. Administratorem danych osobowych zawartych i przetwarzanych w systemach informatycznych Zespołu Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie jest Dyrektor.

2. Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Zespołu Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie, a w szczególności:

   1) zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
   2) zapobiegać przed zabraniem danych przez osobę nieuprawnioną,
   3) zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

3. Do zastosowanych środków technicznych należy:

1) Przetwarzanie danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej.
2) Zabezpieczenie wejścia do pomieszczeń, o których mowa w pkt. 1.
3) Szczególne zabezpieczenie centrum przetwarzania danych (komputer centralny, serwerownia) poprzez zastosowanie systemu kontroli dostępu.
4) Wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji,

4. 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.

5. Niezależnie od niniejszych zasad opisanych w dokumencie "Polityka bezpieczeństwa w Zespole Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie" 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.

6. Wykaz pomieszczeń w których przetwarzane są dane osobowe oraz opis systemów informatycznych Zespołu Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie i ich zabezpieczeń zawiera załącznik nr 1 do niniejszego dokumentu.

7. W celu ochrony przed utratą danych w Zespole Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie stosowane są następujące zabezpieczenia:

   1) Ochrona przed utratą zgromadzonych danych przez robienie kopii zapasowych na nośnikach magnetycznych, z których w przypadku awarii odtwarzane są dane i system operacyjny.
   2) Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Zespołu Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie:
      a) podłączenie danego użytkownika do sieci komputerowej nadzoruje Administrator Bezpieczeństwa Informacji,
      b) aby uzyskać dostęp do zasobów sieci, należy zwrócić się do Administratora Bezpieczeństwa z odpowiednim wnioskiem w którym podane będą dane nowego użytkownika oraz zasoby jakie ma on mieć udostępnione,
      c) w systemie informatycznym Zespołu Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie zastosowano autoryzację użytkownika. Autoryzacji należy dokonać uruchamiając stanowisko komputerowe, podając login użytkownika i hasło.
   3) Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Zespołu Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie poprzez Internet:
      a) zabezpieczenie sieci przed atakiem z zewnątrz poprzez blokowanie wybranych portów,

b) filtrowanie pakietów i blokowanie niektórych usług,
c) objęcie ochroną antywirusową wszystkich danych ściąganych z Internetu na stacjach lokalnych,
d) zapisywanie logów połączeń użytkowników z siecią Internet.

4) Do zabezpieczenia przed wirusami i itp. jest stosowany specjalistyczny program Gdata Anti-Virus.
5) Postanowienia końcowe.

a) do pomieszczeń w których następuje przetwarzanie danych osobowych mają dostęp tylko uprawnione osoby bezpośrednio związane z wykonywanymi czynnościami,
b) zabezpieczenie przed nieuprawnionym dostępem do danych, nadzorowane jest przez Administratora Bezpieczeństwa zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego,
c) w pomieszczeniach w których znajdują się serwery powinna być zapewniona właściwa temperatura i wilgotność powietrza dla sprzętu komputerowego,
d) w pobliżu wejścia do pomieszczenia z serwerami i innym urządzeniami znajduje się gaśnica, która okresowo jest napełniana i kontrolowana przez specjalistę,
e) większość urządzeń w serwerowni umieszczona jest w szafach serwerowych i sieciowych.

ROZDZIAŁ 3

KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Administrator danych, jego zastępca 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.

2. Administrator Bezpieczeństwa sporządza roczny plan kontroli zatwierdzony przez dyrektora i zgodnie z nimi przeprowadza kontrole oraz dokonuje półrocznych ocen stanu bezpieczeństwa danych osobowych.

3. Na podstawie zgromadzonych materiałów, o których mowa w ust. 2, Administrator Bezpieczeństwa sporządza roczne sprawozdanie i przedstawia Administratorowi danych (Dyrektorowi Zespołu Szkół Samochodowych i Budowlanych).

4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Bezpieczeństwa lub osoba go zastępująca:

1) Zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Zespołu Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie.
2) Może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem.
3) Rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora danych.

4) Nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Zespołu Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie.

5. Administrator Bezpieczeństwa dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego załącznik nr 2, który powinien zawierać w szczególności:

   1) Wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem.
   2) Określenie czasu i miejsca naruszenia i powiadomienia.
   3) Określenie okoliczności towarzyszących i rodzaju naruszenia.
   4) Wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania.
   5) Wstępną ocenę przyczyn wystąpienia naruszenia.
   6) Ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

6. Raport, o którym mowa w ust. 5, Administrator Bezpieczeństwa niezwłocznie przekazuje Administratorowi danych (Dyrektorowi Zespołu Szkół Samochodowych i Budowlanych), a w przypadku jego nieobecności osobie uprawnionej.

7. 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.

8. Zaistniałe naruszenie może stać się przedmiotem szczegółowej zespołowej analizy prowadzonej przez Dyrekcję Zespołu Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie, Administratora Bezpieczeństwa Informacji.

9. Analiza, o której mowa w ust. 8, 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 4

POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. W przypadku stwierdzenia naruszenia:

   1) Zabezpieczenia systemu informatycznego.
   2) Technicznego stanu urządzeń.
   3) Zawartości zbioru danych osobowych.
   4) Ujawnienia metody pracy lub sposobu działania programu.
   5) Jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych.
   6) 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>.

2. W razie niemożliwości zawiadomienia Administratora Bezpieczeństwa lub jego zastępcy, należy powiadomić bezpośredniego przełożonego.
3. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Bezpieczeństwa lub jego zastępcy, należy:

    1) 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.
    2) Rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia.
    3) Zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę.
    4) Podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu.
    5) Podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej.
    6) Zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku.
    7) Udokumentować wstępnie zaistniałe naruszenie.
    8) Nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa lub osoby upoważnionej.

ROZDZIAŁ 5

<u>MONITOROWANIE ZABEZPIECZEŃ</u>

1. Prawo do monitorowania systemu zabezpieczeń posiadają zgodnie z zakresem czynności:

    1) Administrator Danych.
    2) Zastępca Administratora Danych, przejmuje obowiązki pod nieobecność Administrator Danych.
    3) Administrator Bezpieczeństwa Informacji.
    4) Zastępca Administratora Bezpieczeństwa Informacji, przejmuje obowiązki pod nieobecność Administrator Bezpieczeństwa Informacji.

2. W ramach kontroli należy zwracać szczególną uwagę na:

    1) Okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do możliwości odtwarzania danych.
    2) Kontrola ewidencji nośników magnetycznych.
    3) Kontrola właściwej częstotliwości zmiany haseł.

ROZDZIAŁ 6

SZKOLENIA

1. Wszyscy pracownicy Zespołu Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie mają obowiązek brać udział w szkoleniach.
2. Szkolenie powinno dotyczyć:

   1) Obowiązujących przepisów i instrukcji wewnętrznych dotyczących ochrony danych osobowych, sposobu niszczenia wydruków i zapisów na nośnikach magnetycznych i optycznych.
   2) Przedstawienie zasad ochrony danych osobowych dotyczących bezpośrednio wykonywanych obowiązków na stanowisku pracy.
   3) Zakresu czynności pracownika zatrudnionego przy przetwarzaniu danych osobowych, którego wzór stanowi załącznik nr 6 do „Polityki bezpieczeństwa".

ROZDZIAŁ 7

NISZCZENIE WYDRUKÓW I ZAPISÓW NA NOŚNIKACH MAGNETYCZNYCH

1. Nośniki magnetyczne przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe.

2. Niszczenie poprzednich zapisów powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.

3. Poprawność przygotowania nośnika magnetycznego powinna być sprawdzona przez Administratora Bezpieczeństwa Informacji.

4. Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć poprzez przecięcie, przełamanie itp.

5. 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 użytkownik stanowiska.

4. Na koniec danego miesiąca wykonywane są kopie bezpieczeństwa z całego programu przetwarzającego dane. Nośniki z kopiami bezpieczeństwa przechowywane są w kasie Zespołu Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie.

5. Kopie awaryjne przechowywane są w szafie pancernej.

6. Nośniki, 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 nadzoruje dokonywanie wymiany kopii awaryjnych na aktualne.

9. Administrator Bezpieczeństwa Informacji nadzoruje okresowo 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 szczegó1ności 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 nadzoruje prowadzenie ewidencji osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego załącznik nr 4 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 (Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zmianami) 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 (Dz.U. z 2002 r. Nr 101, poz. 926 z późn.zmianami), 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).

6. Niniejsza ,,Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Zespole Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie, wchodzi w życie z dniem jej podpisania przez Dyrektora.

Załącznik nr 1 do ,,Polityki bezpieczeństwa”

Wykaz pomieszczeń Zespołu Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie, w których przetwarza się dane osobowe, oraz osoby mające prawo wglądu do danych osobowych.

1. W budynku Zespołu Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie mieszczącego się przy ul. Piastowskiej 2a, znajdują się następujące pomieszczenia w których przetwarza się dane osobowe pracowników oraz uczniów:

1) Pokój – „Sekretariat” – 2 osoby – znajdujący się na parterze budynku ZSSiB.
2) „Pokój nauczycielski” – nauczyciele uczący – znajdujący się na parterze budynku ZSSiB.
3) Pokój „Dyrektor” – 1 osoba – znajdujący się na parterze budynku ZSSiB.
4) Pokój „Zastępców dyrektora” – 3 osoby – znajdujący się na parterze budynku ZSSiB.
5) Pokój ,,Księgowości” – 3 osoby – znajdujący się na parterze w budynku ZSSiB.
6) Pokój „ Pedagogów” – 2 osoby – znajdujący się na I piętrze budynku ZSSiB.
7) Pokój „Biblioteka” –2 osoby – znajdujący się na drugim piętrze budynku ZSSiB.
8) Pokój „Administracji” – 2 osoby – znajdujący się na parterze budynku ZSSiB.

Osoby mające prawo wglądu do danych osobowych w kartotekach z uwagi na wykonywane zakresy czynności	

2. Obsługa techniczna szkoły: sprzątaczki, pracownicy gospodarczy podpisują oświadczenie, którego wzór stanowi załącznik nr 4 do ,,Polityki bezpieczeństwa”.
3. Pracownicy techniczni serwisu zewnętrznego mają wgląd do danych osobowych oraz do systemu informatycznego na podstawie podpisanego oświadczenia, którego wzór stanowi załącznik nr 4 do ,,Polityki bezpieczeństwa”.
4. Osoby odbywające staż, praktykę mają wgląd do danych osobowych oraz do systemu informatycznego na podstawie upoważnienia załącznika Nr 5 nadanego przez Administratora oraz oświadczenia załącznika Nr 4.

Załącznik nr 2 do „Polityki bezpieczeństwa”

R a p o r t
z naruszenia bezpieczeństwa systemu informatycznego w Zespole Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie

1. Data……. Godzina……
/dd.mm.rr./

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

……...
/imię, nazwisko, stanowisko służbowe, nazwa użytkownika – jeśli występuje/

3. Lokalizacja zdarzenia:

……...
/np. nr pokoju, nazwa pomieszczenia/

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

……...

……...

5. Podjęte działania:

……...…
……...

6. Przyczyny wystąpienia zdarzenia:

……...…
……...

7. Postępowanie wyjaśniające:

…….....…
……...

……..……..……
/data, podpis Administratora Bezpieczeństwa Informacji/

Załącznik nr 3 do „Polityki bezpieczeństwa”

Wykaz osób, które zostały zapoznane z „Polityką bezpieczeństwa” systemów informatycznych służących do przetwarzania danych osobowych w Zespole Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie, przeznaczonej dla osób zatrudnionych przy przetwarzaniu tych danych.

Przyjąłem/am do wiadomości i stosowania zapisy Polityki bezpieczeństwa.

Nazwisko i imię	Komórka organizacyjna	Podpis

Załącznik nr 4 do ,,Polityki bezpieczeństwa”

…….
/miejscowość, data/

…….
/imię i nazwisko pracownika/

…….

…….
/adres zamieszkania/

O Ś W I A D C Z E N I E

1. Stwierdzam własnoręcznym podpisem, ze znana jest mi treść przepisów:

   a) o ochronie tajemnic prawnie chronionych stanowiących tajemnicę wynikające z Art.100 § 2 Kodeksu Pracy (Dz.U. z 1998r. Nr 21, poz.94),
   b) o ochronie danych osobowych wynikająca z ustawy o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz.926),
   c) o odpowiedzialności karnej, cywilnej i służbowej za naruszenie ochrony danych osobowych.

2. Zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem/am się w trakcie wykonywanych czynności służbowych.

…… .....……
(podpis pracownika) (podpis złożono w obecności)

Załącznik nr 5 do „Polityki bezpieczeństwa”

……..
/miejscowość, data/

U P O W A Ż N I E N I E N r ……

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101 poz. 926)

U p o w a ż n i a m

……...
/imię i nazwisko/

zatrudnionego na stanowisku ……...

do przetwarzania danych osobowych oraz do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych

w Zespole Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie
/nazwa jednostki organizacyjnej/

Upoważnienie wydaje się na czas zatrudnienia w Zespole Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie

……..
Administrator Danych

Załącznik nr 6 do „Polityki bezpieczeństwa”

…….....
/imię i nazwisko pracownika/

ZAKRES CZYNNOŚCI PRACOWNIKA ZATRUDNIONEGO PRZY PRZETWARZANIU DANYCH OSOBOWYCH

I. Obowiązki pracownika

Pracownik dopuszczony do przetwarzania danych osobowych zobowiązany jest do:

1. Zapoznania się i wypełniania obowiązków wynikających z :
   - przepisów ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.) oraz przepisów wykonawczych wydanych na jej podstawie,
   - przepisów Konwencji oraz Dyrektyw dotyczących ochrony danych osobowych, w tym Dyrektywy 95/46/WE Parlamentu Europejskiego I Rady z dnia 24 października 1995r. w sprawie ochrony danych osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

2. Kontrolowania dostępu do danych osobowych.

3. Zachowania w tajemnicy danych oraz sposobu ich zabezpieczania do których uzyskał dostęp w trakcie zatrudnienia, również po ustaniu zatrudnienia.

4. Zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem.

II. Odpowiedzialność pracownika

Za niedopełnienie obowiązków wynikających z niniejszego aneksu pracownik ponosi odpowiedzialność na podstawie przepisów Regulaminu pracy, Kodeksu pracy oraz Ustawy o ochronie danych osobowych.

Oświadczam, że treść niniejszego zakresu jest mi znana i zobowiązuję się do jego przestrzegania.

Potwierdzam odbiór 1 egz. zakresu czynności dot. przetwarzania danych osobowych.

…… ……
/podpis pracodawcy/ /podpis pracownika/

ZARZĄDZENIE Nr 0133-19a/09

DYREKTORA ZESPOŁU SZKÓŁ SAMOCHODOWYCH I BUDOWLANYCH

IM. LEONARDA DA VINCI W GŁOGOWIE

z dnia 20 sierpnia 2009 roku

w sprawie ustanowienia Administratora Bezpieczeństwa Informacji

Na podstawie art.36 ust.3 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 ze zm.)

u s t a n a w i a m

z dniem 1 września 2009 roku

Pana Tomasza Cierniaka

ADMINISTRATOREM BEZPIECZEŃSTWA INFORMACJI

w Zespole Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie .

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

Załącznik do Zarządzenia Nr 0133-19a/09 Dyrektora Zespołu Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie z dnia 20 sierpnia 2009r.

Zakres czynności Administratora Bezpieczeństwa Informacji w Zespole Szkół Samochodowych i Budowlanych im Leonarda da Vinci w Głogowie.

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 w uzgodnieniu z kierownikiem zespołu administracyjnego 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. Nadzór nad 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 w uzgodnieniu z kierownikiem zespołu administracyjnego nad obiegiem dokumentów zawierających dane osobowe.

8. Nadzór nad prawidłowością archiwizacji oraz usuwania danych osobowych.

9. Monitorowanie funkcjonowania zabezpieczeń wdrożonych w celu ochrony danych osobowych.

10. Wdrożenie szkoleń z zakresu przepisów dotyczących ochrony danych oraz stosowania środków technicznych i organizacyjnych przy przetwarzaniu danych w systemach informatycznych.

Zarządzenie nr 0133-19/09 Dyrektora Zespołu Szkół Samochodowych i Budowlanych im. Leonarda da Vinci z dnia 20 sierpnia 2009r.

w sprawie dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki technicznych i organizacyjne zapewniające ochronę przetwarzanych danych osobowych

Zgodnie z Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., Nr 100, poz. 1024) wprowadzam jako obowiązującą w Zespole Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie dokumentację Systemu Zarządzania Bezpieczeństwem Baz Danych, której integralną częścią są:

§ 1. Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Zespole Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie.

§ 2. Zobowiązanie pracowników Zespołu Szkół Samochodowych i Budowlanych im. Leonarda da Vinci w Głogowie do stosowania zasad określonych w ,,Polityce bezpieczeństwa”

§ 3. Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 4. Zarządzenie wchodzi w życie od dnia 1 września 2009r.

.....
podpis dyrektora