„ZATWIERDZAM"

DYREKTOR
ZESPOŁU SZKÓŁ ZAWODOWYCH
mgr Barbara Tetla-Gruszczyk

REGULAMIN OCHRONY DANYCH OSOBOWYCH

ZESPOŁU SZKÓŁ ZAWODOWYCH W JASTRZĘBIU-ZDROJU

Administrator Bezpieczeństwa

Informacji

Przemysław Drozd

Jastrzębie-Zdrój 2011

ZESPÓŁ SZKÓŁ ZAWODOWYCH
ul. 11 Listopada 45
44-330 Jastrzębie-Zdrój
tel. 32/ 47 620-71
NIP 633-183-82-37 REGON 273067490

Za zgodność z oryginałem
2015 -03- 13
data podpis

DYREKTOR
ZESPOŁU SZKÓŁ ZAWODOWYCH
mgr Barbara Tetla-Gruszczyk

SPIS TREŚCI

I. POLITYKA BEZPIECZEŃSTWA

POJĘCIA PODSTAWOWE

1. Polityka Bezpieczeństwa została utworzona w związku z wymaganiami zawartymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926, ze zm.) oraz rozporządzeniu 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. Opracowany dokument jest zgodny z dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osób oraz ochrony prywatności w sektorze komunikacji elektronicznej.

2. Regulamin niniejszy określa tryb i zasady ochrony danych osobowych przetwarzanych w Zespole Szkół Zawodowych , zwanym dalej Jednostką.

3. Ilekroć w regulaminie jest mowa o :

   a) **Jednostce** – rozumie się przez to Zespół Szkół Zawodowych;

   b) **zbiorze danych osobowych** - 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;

   c) **danych osobowych** - rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

   d) **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;

   e) **systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;

   f) **systemie tradycyjnym** - rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;

   g) **zabezpieczeniu danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

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

i) **administratorze danych osobowych** - w świetle art. 3 i 7 pkt 4 ustawy o ochronie danych osobowych rozumie się przez to Dyrektora Jednostki, który decyduje o celach i środkach przetwarzania danych osobowych;

j) **administratorze bezpieczeństwa informacji**- rozumie się przez to osobę wyznaczoną przez Dyrektora Jednostki, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;

k) **administratorze systemu informatycznego** - rozumie się przez to osobę zatrudnioną przez Dyrektora Jednostki, upoważnioną do realizacji zadań związanych z zarządzaniem systemem informatycznym;

l) **użytkowniku systemu informatycznego** - rozumie się przez to upoważnionego przez Dyrektora Jednostki, wyznaczonego do przetwarzania danych osobowych w systemie informatycznym pracownika, który odbył stosowne szkolenie w zakresie ochrony tych danych;

m) **zgodzie osoby, której te dane dotyczą** - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie - zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

CELE

Celem opracowania polityki bezpieczeństwa jest ochrona przed niepowołanym dostępem do:

a) systemu informatycznego oraz informacji udostępnianych z jego wykorzystaniem;

b) informacji zgromadzonych, przetwarzanych w formie tradycyjnej.

Niniejsze opracowanie określa politykę bezpieczeństwa w zakresie przetwarzania danych osobowych przez pracowników Jednostki, a w szczególności Kierowników/Dyrektorów komórek organizacyjnych oraz administratorów systemów informatycznych.

Dane osobowe w Jednostce są gromadzone, przechowywane, edytowane, archiwizowane w kartotekach, skorowidzach, księgach, wykazach, zestawieniach oraz w innych zestawach i zbiorach ewidencyjnych poszczególnych komórek organizacyjnych Jednostki na dokumentach papierowych, jak również w systemach informatycznych na elektronicznych nośnikach informacji.

Powyższy dokument wprowadza regulacje w zakresie zasad organizacji procesu przetwarzania i odnosi się swoją treścią do informacji

a) w formie papierowej - przetwarzanej w ramach SYSTEMU TRADYCYJNEGO ;

b) w formie elektronicznej - przetwarzanej w ramach SYSTEMU INFORMATYCZNEGO;

Bezpośredni nadzór nad przetwarzaniem danych osobowych sprawują Kierownicy komórek organizacyjnych.

Z zapisanymi w polityce bezpieczeństwa obowiązkowo są zapoznawani wszyscy użytkownicy systemów informatycznych i tradycyjnych.

Do informacji przechowywanych w systemach informatycznych jak i dokumentów tradycyjnych mają dostęp jedynie upoważnieni pracownicy Jednostki oraz osoby mające imienne zarejestrowane upoważnienie. Wszyscy pracownicy zobowiązani są do zachowania tych danych w tajemnicy. Dopuszczalny sposób i zakres przetwarzania danych osobowych regulują zapisy ustaw kompetencyjnych, szczegółowych właściwych dla komórek organizacyjnych Jednostki.

Dane osobowe są chronione zgodnie z polskim prawem oraz procedurami obowiązującymi w instytucjach samorządowych dotyczącymi bezpieczeństwa i poufności przetwarzanych danych. Systemy informatyczne oraz tradycyjne, które przechowują dane osobowe, są chronione odpowiednimi środkami technicznymi. Opracowane procedury określają obowiązki użytkownika zbiorów tradycyjnych oraz zasady korzystania z systemów informatycznych. Każdy użytkownik systemu informatycznego zobowiązany jest zapamiętać swoją nazwę użytkownika oraz hasło i nie udostępniać go innym osobom. Użytkownik systemu informatycznego powinien pamiętać o wylogowaniu się po zakończeniu korzystania z usług systemów informatycznych.

II. ADMINISTRACJA I ORGANIZACJA BEZPIECZEŃSTWA

INFORMACJE OGÓLNE

Za bezpieczeństwo danych osobowych przetwarzanych w systemach przetwarzania danych osobowych odpowiada administrator danych osobowych. Kierownicy komórek organizacyjnych obowiązani są zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinni zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą utratą uszkodzeniem lub zniszczeniem.

Administrator danych może wyznaczyć administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony. Prowadzi on dokumentację opisującą sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych.

ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

Administrator Bezpieczeństwa Informacji wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemami informatycznymi i tradycyjnymi.

Administrator Bezpieczeństwa Informacji jest zobowiązany do zapewnienia, poprzez zastosowanie odpowiednich środków i metod kontroli dostępu, iż wyłącznie autoryzowany personel ma dostęp do systemów informatycznych i tradycyjnych. Ponadto, w uzgodnieniu z kierownikami komórek organizacyjnych, określa warunki oraz sposób przydzielania użytkownikom kont i haseł. Administrator Bezpieczeństwa Informacji posiada bieżącą listę osób upoważnionych do przetwarzania danych osobowych.

Szczegółowy zakres odpowiedzialności i obowiązków Administratora Bezpieczeństwa Informacji jest następujący:

a) nadzoruje bezpieczeństwo systemów informatycznych i tradycyjnych;

b) nadzoruje przestrzeganie przez wszystkich użytkowników stosowanie obowiązujących procedur;

c) weryfikuje listę autoryzowanych użytkowników systemów informatycznych;

d) doradza użytkownikom w zakresie bezpieczeństwa;

e) zapewnia, aby cały personel posiadający dostęp do systemu posiadał stosowne zezwolenia oraz był przeszkolony w zakresie obowiązujących regulacji bezpieczeństwa;

f) przygotowuje i prowadzi „Ewidencja osób biorących udział w przetwarzaniu danych osobowych";

g) prowadzi kontrole w zakresie bezpieczeństwa;

h) przygotowuje wnioski pokontrolne dla Administratora.

ADMINISTRATOR SYSTEMU INFORMATYCZNEGO

Administrator systemu informatycznego wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemem informatycznym. Jest zobowiązany do zapewnienia, poprzez zastosowanie odpowiednich środków i metod kontroli dostępu, w taki sposób, że wyłącznie autoryzowany personel ma dostęp do systemów informatycznych. Przydziela użytkownikom systemu informatycznego konta i hasła. Ewidencjonuje użytkowników systemu.

Szczegółowy zakres odpowiedzialności i obowiązków Administratora Systemu Informatycznego jest następujący:

a) odpowiada za bezpieczeństwo systemu informatycznego;

b) zobowiązuje i bieżąco kontroluje stosowanie się użytkowników do obowiązujących procedur;

c) utrzymuje i aktualizuje listę autoryzowanych użytkowników systemu informatycznego;

d) zapewnia aktualizację dokumentacji technicznej systemu w tym opis struktur zbiorów i ich zależności.

UŻYTKOWNIK SYSTEMU

Użytkownik systemu wykonuje wszystkie prace niezbędne do efektywnej oraz bezpiecznej pracy na stanowisku pracy również z wykorzystaniem stacji roboczej. Jest odpowiedzialny przed Administratorem Bezpieczeństwa Informacji za nadzór, implementację i utrzymanie niezbędnych warunków bezpieczeństwa w szczególności do przestrzegania procedur dostępu do systemu i ochrony danych osobowych.

POZIOM BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMIE INFORMATYCZNYM

Do grupy danych osobowych przetwarzanych w Jednostce jako pojedyncze informacje, w zestawach lub zbiorach w postaci papierowej ustala się zabezpieczenia na poziomie niskim.

Do grupy danych osobowych przetwarzanych w systemach informatycznych, ustala się zabezpieczenia na poziomie wysokim

PROCEDURY DOSTĘPU DO SYSTEMU

1. Procedury dostępu do systemów tradycyjnych

Lp.	*Czynność*	*Podstawa*	*Kto*	*Uwagi*

2. Procedury dostępu do systemów informatycznych :

Lp.	*Czynność*	*Podstawa*	*Kto*	*Uwagi*

III. WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

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 aplikacje (programy):

Zestawienie programów oraz zbiorów stanowi załącznik do polityki bezpieczeństwa.

IV. OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I POWIĄZANIA MIĘDZY NIMI

1. Zbiory danych osobowych w Jednostce podzielone są funkcjonalnie (zestawienie zbiorów przetwarzanych w Jednostce stanowi załącznik nr 3 do Regulaminu Ochrony Danych Osobowych). Gromadzi się je, przechowuje i przetwarza tradycyjnie na nośnikach papierowych, jak również w systemie informatycznym, w zakresie:

   a) akt osobowych :

   - kandydatów do pracy;
   - pracowników aktualnie zatrudnionych (niezależnie od rodzaju umowy);
   - byłych pracowników (zwolnionych);
   - osób odbywających staż;
   - absolwentów gimnazjum przyjmowanych do szkoły
   - uczniów szkoły

   b) kartotek:

   - płacowych
   - list płac
   - obsługi księgowej

2. Ze względu na rodzaj i charakter danych osobowych zawartych w zbiorach, w Urzędzie wyróżnia się dwie kategorie danych:

   - **dane osobowe zwykłe** - wszelkie dane (informacje) dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, zgromadzone w zbiorach danych osobowych wymienionych w IV.1.;
   - **dane osobowe sensytywne** – zgodnie z katalogiem zawartym w treści Ustawy o Ochronie Danych Osobowych art. 27 ust 1. wszelkie dane (informacje) ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne, przynależność partyjną lub związkową, jak również informacje o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym

3. Zgodnie z postanowieniami art. 40 ustawy o ochronie danych osobowych, z uwagi na gromadzone kategorie zbiorów danych osobowych Jednostka Zespołu szkól Zawodowych jest zwolniona z obowiązku zgłoszenia i rejestracji tych zbiorów u Generalnego Inspektora Ochrony Danych Osobowych.

V. SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

1. Komunikacja :

   - **obieg** dokumentów zawierających dane osobowe, pomiędzy komórkami organizacyjnymi Jednostki, winien odbywać w sposób zapewniający pełną ochronę przed ujawnieniem zawartych w tych dokumentach danych (informacji).

2. Komunikacja w sieci komputerowej:

   Przekazywanie informacji (danych) w systemie informatycznym poza sieć lokalną Jednostki odbywa się w relacji:

   Jednostka - mieszkańcy, przedsiębiorcy, kontrahenci, Zakład Ubezpieczeń Społecznych, Urząd Skarbowy, Banki, Narodowy Fundusz Ochrony Zdrowia, Urząd Wojewódzki, Urząd Marszałkowski inne komórki samorządowe i rządowe.

   Zabronione jest jednoczesne podłączanie komputerów do sieci wewnętrznej Zespołu Szkół Zawodowych i sieci zewnętrznych (Plus , Era , Orange , WiFi , WiMAX itp.).

VI. OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

Dostęp do danych wprowadzonych przez użytkowników systemów informatycznych mają jedynie upoważnieni pracownicy zespołu orzekającego oraz administrator systemu zapewniający jego prawidłową eksploatację. Wszyscy pracownicy, będący użytkownikami systemu zobowiązani są do zachowania tych danych w tajemnicy.

a) Ochronie podlegają dane osobowe gromadzone i przetwarzane w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych oraz w urządzeniach i systemie informatycznym Jednostki;

b) Pomieszczenia, w których przetwarza się dane osobowe powinny być fizycznie zabezpieczone przed dostępem osób nieuprawnionych, to znaczy posiadać odpowiednie zamki do drzwi, zabezpieczenia w oknach (w szczególności na parterze) oraz być wyposażone w środki ochrony ppoż.

c) Dokumenty i nośniki informacji, zawierające dane osobowe powinny być zabezpieczone przed dostępem osób nieupoważnionych do przetwarzania danych. Jeśli nie są aktualnie używane powinny być przechowywane w szafach lub w innych przeznaczonych do tego celu urządzeniach biurowych, posiadających odpowiednie zabezpieczenia :

Zasady zabezpieczania danych:

- zbiory kartotekowe winny znajdować się w pomieszczeniach zabezpieczonych przed dostępem osób nieupoważnionych;
- szafy zamykane na klucz
- szafy metalowe
- kraty w oknach
- alarm
- rolety antywłamaniowe w drzwiach gabinetów
- monitoring obiektu

VII. UDOSTĘPNIANIE POSIADANYCH W ZBIORZE DANYCH OSOBOWYCH

1) Do udostępniania posiadanych w zbiorze danych osobowych upoważniony jest dyrektor Zespołu Szkół Zawodowych (administrator danych osobowych) lub pracownik posiadający wymagane prawem upoważnienie.

2) W przypadku udostępniania danych osobowych w celach innych niż włączenie do zbioru, administrator danych udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

VIII. BEZPIECZEŃSTWO PERSONELU

INFORMACJE OGÓLNE

Należy mieć świadomość, że każdy, kto ma dostęp do pomieszczenia, w którym zainstalowano sprzęt systemu informatycznego może spowodować jego uszkodzenie lub może mieć dostęp do informacji wyświetlanych na monitorze lub wydruków.

Zagrożenia w stosunku do systemu mogą pochodzić również od każdej innej osoby np. personelu pomocniczego, technicznego, konsultanta itp., posiadającej wystarczające umiejętności i wiedzę, aby uzyskać dostęp do sieci.

UŻYTKOWNICY SYSTEMU

Wszyscy użytkownicy systemu muszą stosować się do obowiązujących procedur bezpieczeństwa.

Hasło podlega szczególnej ochronie. Użytkownik ma obowiązek tworzenia haseł o długości min. 8 znaków, nie trywialnych, tzn. nie może używać imion, danych identyfikujących użytkownika oraz jego najbliższych, numerów rejestracyjnych, marek lub typów swoich samochodów itp., oraz nie może tworzyć haseł przez kombinację tych nazw lub ich zmianę uporządkowania np. od tyłu. Jest wprowadzony wymóg zabraniający dokonywana zapisów haseł przez użytkowników. W przypadku, gdy użytkownik zapomni swoje hasło, może on uzyskać nowe hasło od Administratora Systemu zgodnie z obowiązująca procedurą

IX. BEZPIECZEŃSTWO FIZYCZNE

INFORMACJE OGÓLNE

Informacja przetwarzana i przechowywana w systemie musi być zabezpieczona w szczególny sposób.

Środki bezpieczeństwa fizycznego są konieczne dla zapobiegania niepowołanemu dostępowi do informacji, nieautoryzowanym operacjom w systemie, kontroli dostępu do zasobów oraz w celu zabezpieczenia sprzętu teleinformatycznego.

POMIESZCZENIA LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE - OBSZAR SYSTEMU -

Obszar systemów informatycznych w Urzędzie obejmuje wszystkie pomieszczenia budynków Urzędu.

Pomieszczenia te zabezpieczone są w następujący sposób: portier, firma ochroniarska, zamki patentowe

OCHRONA SERWERA, STACJI ROBOCZYCH I NOŚNIKÓW

Pomieszczenia, w których znajdują się stanowiska komputerowe są:

a) zamknięte, jeśli nikt w nich nie przebywa;

b) wyposażone w sejfy lub inne pojemniki umożliwiające przechowywanie dokumentów.

.....

ZASADY KONTROLI SPRZĘTU

Instalacja urządzeń systemu i sieci teleinformatycznej odbywa się za wiedzą i pod kontrolą Dyrektora komórki organizacyjnej, który jest również odpowiedzialny za warunki wprowadzania do użycia, przechowywania, eksploatacji oraz wycofywania z użycia każdego urządzenia.

X. BEZPIECZEŃSTWO SPRZĘTU I OPROGRAMOWANIA

INFORMACJE OGÓLNE

Sprzęt i oprogramowanie, indywidualnie lub łącznie mają ścisły związek z bezpieczeństwem systemu i sieci teleinformatycznej. Dlatego, powinny być ściśle przestrzegane procedury bezpieczeństwa odnoszące się do tych elementów.

BEZPIECZEŃSTWO SPRZĘTOWE

Sieć teleinformatyczna jest organizacyjnym i technicznym połączeniem systemów teleinformatycznych wraz z łączącymi je urządzeniami i liniami telekomunikacyjnymi. Niedopuszczalne jest samowolne przemieszczanie lub zmiana konfiguracji stacji roboczej bez wiedzy kierownika/dyrektora komórki organizacyjnej.

BEZPIECZEŃSTWO OPROGRAMOWANIA

Nie zezwala się na korzystanie z jakiegokolwiek nowego oprogramowania bez zgody Administratora Systemu. Dodatkowe oprogramowanie może być instalowane wyłącznie po uzyskaniu zezwolenia Administratora Systemu. Kopie oprogramowania operacyjnego, aplikacyjnego i użytkowego przechowuje się w serwerowni.

Używanie oprogramowania prywatnego w sieci jest kategorycznie zabronione. Na stacjach roboczych powinno być zainstalowane jedynie niezbędne oprogramowanie.

XI. KONSERWACJE I NAPRAWY

KONSERWACJA SPRZĘTU

Każde urządzenie użytkowane w systemie informatycznym, powinno podlegać rutynowym czynnościom konserwacyjnym oraz przeglądom wykonywanym przez uprawnione osoby.

KONSERWACJA OPROGRAMOWANIA

Za konserwację oprogramowania systemowego oraz aplikacyjnego serwera systemu informatycznego odpowiedzialny jest Administrator Systemu. Konserwacja ww. oprogramowania obejmuje także jego aktualizację.

Za konserwację oprogramowania stanowisk roboczych odpowiedzialny jest kierownik/dyrektor komórki organizacyjnej. Wszelkie aktualizacje oprogramowania powinny być uzgadniane z Administratorem Systemu

NAPRAWA SPRZĘTU

Administrator Systemu przed rozpoczęciem naprawy urządzenia przez zewnętrzne firmy sprawdza, czy spełnione są następujące wymagania:

a) w przypadku awarii serwera i konieczności oddania sprzętu do serwisu, nośniki magnetyczne zawierające dane osobowe powinny być wymontowane i do czasu naprawy serwera przechowywane w szafie metalowej znajdującej się w strefie o ograniczonym dostępie;

b) w przypadku uszkodzenia nośnika magnetycznego zawierającego dane osobowe należy komisyjnie dokonać jego zniszczenia.

XII. PLANY AWARYJNE I ZAPOBIEGAWCZE

ZASILANIE

Serwer systemu oraz poszczególne stacje robocze (opcjonalnie) powinny być zabezpieczone urządzeniami podtrzymującymi zasilanie (UPS), co umożliwi funkcjonowanie systemu w przypadku awarii zasilania.

KOPIE ZAPASOWE

W celu zabezpieczenia ciągłości pracy, informacja przechowywana i przetwarzana w systemie podlega codziennej, przyrostowej archiwizacji (opcjonalnie) oraz pełnej archiwizacji przeprowadzanej nie rzadziej niż raz na dwa tygodnie. Kopie archiwalne danych są wykonywane na nośnikach magnetooptycznych, i przechowywane są przez Administratora Systemu. Użycie kopii zapasowych następuje na polecenie Administratora Systemu w przypadku odtwarzania systemu po awarii.

XIII. POLITYKA ANTYWIRUSOWA

W zakresie ochrony antywirusowej wprowadza się następujące zalecenia:

a) nie należy używać oprogramowania na stacji roboczej innego niż zaleca administrator systemu;

b) nie wolno instalować oprogramowania typu freeware czy shareware;

c) regularnie uaktualniać bazę wirusów zainstalowanego oprogramowania antywirusowego;

d) przed użyciem nośnika danych sprawdzić czy nie jest zainfekowany wirusem komputerowym.

POSTĘPOWANIE W PRZYPADKU WYKRYCIA WIRUSA

natychmiastowe powiadomienie administratora bezpieczeństwa informacyjnego. Podjęcie działań przez Administratora Systemu w celu usunięcia wirusa po otrzymaniu powiadomienia.

XIV. ZALECENIA ORGANIZACYJNE

.....

XV. WYKAZ PODSTAWOWYCH AKTÓW PRAWNYCH MOGĄCYCH MIEĆ ZASTOSOWANIE W ZAKRESIE GROMADZENIA, PRZETWARZANIA I PRZEKAZYWANIA DANYCH OSOBOWYCH W URZĘDZIE MIASTA TARNOWA

1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 101, póz. 926 z dnia 6 lipca 2002 r. z późn. zmianami);

2. 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. Nr 100, póz. 1024z2004r);

3. Ustawa z dnia 22 stycznia 2004 r. o zmianie ustawy o ochronie danych osobowych (Dz. U. Nr 33, póz. 285 z dnia 2 marca 2004 r.);

4. Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika (Dz. U. z dn.1.06.1996r Nr62, póz. 286-z późn. zmianami);

5. Ustawa z dnia 26 czerwca 1974r Kodeks pracy (Dz. U. z dn. 5.07.1974r Nr 24, póz. 1 z późn. zmianami);

6. Ustawa z dnia 13 października 1998r o systemie ubezpieczeń społecznych (Dz.U. zdn. 10.11.1998r Nr 137, póz. 887 z późn. zmianami);

7. Ustawa z dnia 29 sierpnia 1997r Ordynacja podatkowa (Dz.U. z1997r Nr 137, póz. 926 z późn. zmianami);

8. Ustawa z dnia 29 sierpnia 1997r Prawo bankowe (Dz.U. z 1997r Nr 140, póz. 939 z późn. zmianami);

9. Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2001r, Nr 142, póz. 1591 z późn. zmianami).

XVI. LISTA ZAŁĄCZNIKÓW

1. Wykaz budynków
2. Oświadczenie
3. Wykaz osób zapoznanych z Regulaminem Ochrony Danych Osobowych
4. Ewidencja osób upoważnionych do przetwarzania danych osobowych
5. Wykaz administratorów systemów informatycznych

Załącznik nr ....1....

„ZATWIERDZAM"

DYREKTOR
ZESPOŁU SZKÓŁ ZAWODOWYCH
mgr Barbara Tetla-Gruszczyk

WYKAZ BUDYNKÓW ZESPOŁU SZKÓŁ ZAWODOWYCH W JASTRZĘBIU-ZDROJU

Stan na dzień: 30.09.2011 r.

Numer wersji: 1

Administrator Bezpieczeństwa Informacji

Przemysław Drozd

Jastrzębie-Zdrój

1. Zespół Szkół Zawodowych ul. 11 Listopada 45 Jastrzębie-Zdrój

Załącznik nr ..5..

„ZATWIERDZAM"

DYREKTOR
ZESPOŁU SZKÓŁ ZAWODOWYCH
mgr Barbara Tetla-Gruszczyk

WYKAZ ADMINISTRATORÓW SYSTEMÓW INFORMATYCZNYCH

ZESPOŁU SZKÓŁ ZAWODOWYCH W JASTRZĘBIU- ZDROJU

Stan na dzień: 30.09.2011 r

Numer wersji: 1

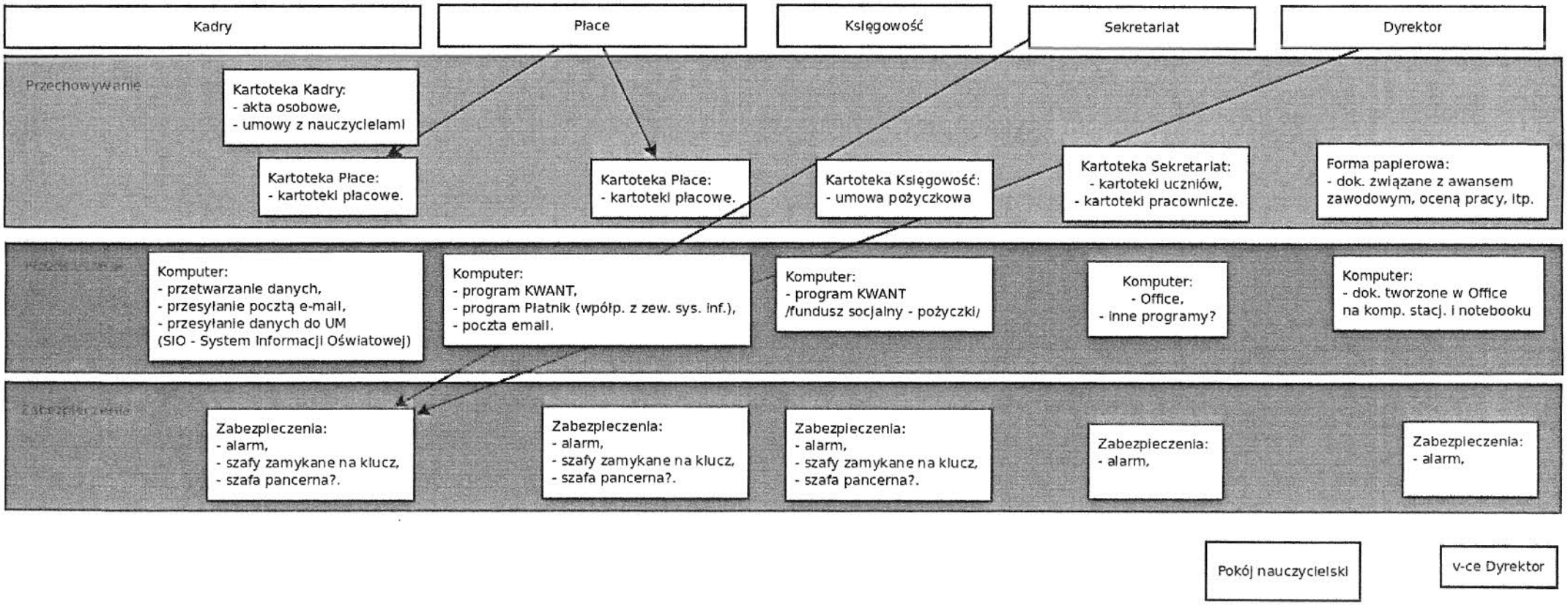
Administrator Bezpieczeństwa Informacji

Przemysław Drozd

2011 rok

LISTA ADMINISTRATORÓW SYSTEMÓW INFORMATYCZNYCH

1. Przemysław Drozd


Kadry
Płace
Księgowość
Sekretariat
Dyrektor
Przechowywanie
Kartoteka Kadry:
- akta osobowe,
- umowy z nauczycielami
Kartoteka Płace:
- kartoteki płacowe.
Kartoteka Płace:
- kartoteki płacowe.
Kartoteka Księgowość:
- umowa pożyczkowa
Kartoteka Sekretariat:
- kartoteki uczniów,
- kartoteki pracownicze.
Forma papierowa:
- dok. związane z awansem zawodowym, oceną pracy, itp.
Komputer:
- przetwarzanie danych,
- przesyłanie pocztą e-mail,
- przesyłanie danych do UM
(SIO - System Informacji Oświatowej)
Komputer:
- program KWANT,
- program Płatnik (współp. z zew. sys. inf.),
- poczta email.
Komputer:
- program KWANT
/fundusz socjalny - pożyczki/
Komputer:
- Office,
- inne programy?
Komputer:
- dok. tworzone w Office
na komp. stacj. i notebooku
Zabezpieczenia:
- alarm,
- szafy zamykane na klucz,
- szafa pancerna?.
Zabezpieczenia:
- alarm,
- szafy zamykane na klucz,
- szafa pancerna?.
Zabezpieczenia:
- alarm,
- szafy zamykane na klucz,
- szafa pancerna?.
Zabezpieczenia:
- alarm,
Zabezpieczenia:
- alarm,
Pokój nauczycielski
v-ce Dyrektor

Wykaz przetwarzanych zbiorów danych

Tabela 1

Nazwa zbioru danych	Forma prowadzenia zbioru	Środowisko pracy	Zawartość pól informacyjnych (zakres danych)	Jednostki organizacyjne wykorzystujące zbiór	Lokalizacja zbioru danych	Inne aplikacje , z którymi komunikuje się i wymienia dane	Nazwa serwera Adres IP	Administrator aplikacji

Upoważnienie

uprawniające użytkowników systemu informatycznego, w którym przetwarzane są dane osobowe, do przetwarzania tych danych

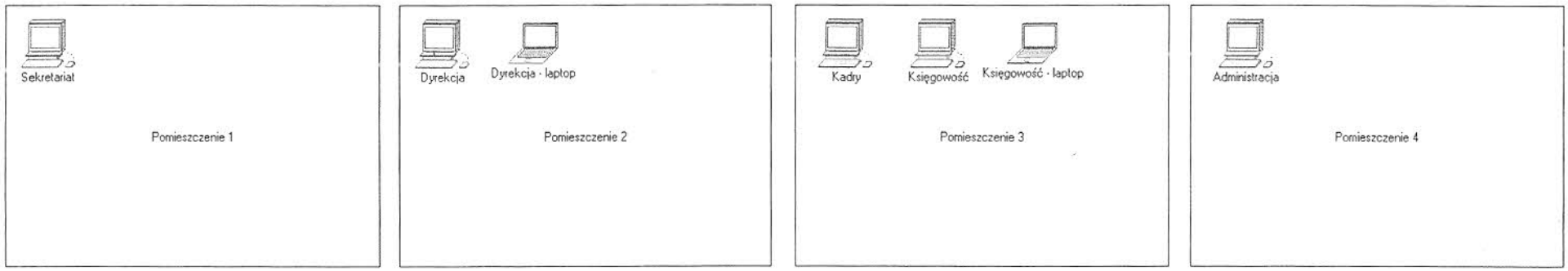
Niniejszym upoważniam Panią ..... do przetwarzania danych osobowych w systemie informatycznym Zespołu Szkół Zawodowych.

Administrator danych: .....

Administrator bezpieczeństwa danych: .....

data: .....

Wykaz pomieszczeń, w których przetwarzane są dane osobowe



Sposób przepływu danych pomiędzy poszczególnymi systemami informatycznymi