Zarządzenie Nr 16 /2013
Dyrektora Miejskiego
Oświatowego Zespołu Ekonomicznego w Tarnobrzegu
z dnia 22.11.2013
w sprawie ochrony przetwarzanych danych osobowych
w Miejskim Oświatowym Zespole Ekonomicznym
w Tarnobrzegu

Na podstawie art. 36 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.) oraz w oparciu
o treść 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. z 2004 r. Nr 100, poz. 1024). Zarządzam co następuje :

§ 1

Ustalam dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych.

§ 2

Na dokumentację, o której mowa w § 1 składa się:

1) polityka bezpieczeństwa stanowiąca Załącznik Nr 1 do niniejszego Zarządzenia,
2) instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, stanowiąca Załącznik Nr 2 do Zarządzenia,

3) polityka bezpieczeństwa przetwarzania danych osobowych, stanowiąc Załącznik Nr 3 Zarządzenia.

§ 3

Wykonanie Zarządzenia powierza się Dyrektorowi Miejskiego Oświatowego Zespołu Ekonomicznego w Tarnobrzegu.

§ 4

Zarządzenie obowiązuje od dnia 02.04.2013 r.

Dyrektor Miejskiego Oświatowego
Zespołu Ekonomicznego w Tarnobrzegu

Małgorzata Mazurek

Załącznik Nr 1 do Zarządzenia Nr 16/2013
Dyrektora Miejskiego Oświatowego Zespołu Ekonomicznego
w Tarnobrzegu z dnia 22.11.2013

POLITYKA BEZPIECZEŃSTWA INFORMACJI I OCHRONY DANYCH OSOBOWYCH MIEJSKIEGO OŚWIATOWEGO ZESPOŁU EKONOMICZNEGO W TARNOBRZEGU

Spis treści

Rozdział I

POSTANOWIENIA OGÓLNE

§1

1. Administrator Danych ma świadomość znaczenia przetwarzanych informacji dla realizacji celów jednostki i potrzeby ochrony informacji, poprzez budowę systemu zarządzania bezpieczeństwem informacji.

2. Zasady, działania, kompetencje i zakresy odpowiedzialności opisane w niniejszej Polityce Bezpieczeństwa Informacji obowiązują wszystkich pracowników Administratora Danych.
3. Procedury i dokumenty związane z Polityką Bezpieczeństwa Informacji będą weryfikowane i dostosowywane w celu zapewnienia odpowiedniego poziomu bezpieczeństwa. Przeglądy dokumentacji odbywają się nie rzadziej niż raz w roku.
4. Polityka bezpieczeństwa informacji i ochrony danych osobowych zwana dalej „Polityką", określa środki techniczne i organizacyjne zastosowane przez Administratora Danych dla zapewnienia ochrony danych oraz tryb postępowania w przypadku stwierdzenia naruszenia zabezpieczenia danych w systemie informatycznym lub w kartotekach, albo
w sytuacji podejrzenia o takim naruszeniu.
5. Polityka została opracowana zgodnie z wymogami obowiązujących przepisów w zakresie ochrony informacji i danych osobowych, ze szczególnym uwzględnieniem Ustawy
o ochronie danych osobowych, oraz obowiązujących aktów prawnych dotyczących oświaty, nauki, wychowania.

§ 2

1. Ilekroć w Polityce jest mowa o:

1) Administratorze Danych - rozumie się przez to Miejski Oświatowy Zespół Ekonomiczny w Tarnobrzegu, reprezentowany przez Dyrektora.
2) 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,
3) kartotece – rozumie się przez to zewidencjonowany, usystematyzowany zbiór wykazów, skoroszytów, wydruków komputerowych i innej dokumentacji gromadzonej
w formie papierowej, zawierającej dane osobowe
4) przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

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

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

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

8) Administratorze Bezpieczeństwa Informacji, zwanego dalej „ABI" – rozumie się przez to osobę nadzorującą przestrzeganie zasad ochrony przetwarzanych danych osobowych i informacji prawem chronionych. Nadzoruje on stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz zmianą, utratą, uszkodzeniem, lub zniszczeniem, a także przeprowadza kontrole w zakresie określonym regulacjami wewnętrznymi Administratora Danych.

Administratora bezpieczeństwa informacji wyznacza Administrator danych.

Wyznaczenie ABI opisuje załącznik nr 1 do niniejszej Polityki.

9) Administratorze Systemu Informatycznego – rozumie się przez to osobę odpowiedzialną za prawidłowe funkcjonowanie sprzętu, oprogramowania i jego konserwację, za techniczno-organizacyjną obsługę systemu teleinformatycznego, zwanego dalej „Informatykiem". Wyznaczenie Informatyka opisuje załącznik nr 2 do niniejszej Polityki.

10) użytkowniku – rozumie się przez to osobę upoważnioną przez Administratora Danych do przetwarzania informacji i danych osobowych.

11) komórce organizacyjnej – rozumie się przez to każdą wydzieloną organizacyjnie i funkcjonalnie komórkę wewnętrzną, zgodnie z podziałem przeprowadzonym przez Administratora Danych. Schemat organizacji nadzoru zasad ochrony danych opisuje załącznik nr 6.

12) pomieszczeniach – rozumie się przez to budynki i pomieszczenia określone przez Administratora Danych, tworzące obszar, w którym przetwarzane są dane osobowe i inne informacje prawem chronione.

Obszar przetwarzania danych podany jest w załączniku nr 3 do niniejszej Polityki.

§ 3

1. W celu zwiększenia efektywności ochrony informacji dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Ochrona

informacji jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.

2. Zastosowane zabezpieczenia mają służyć osiągnięciu poniższych celów i zapewnić:

1) rozliczalność – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

2) integralność – rozumie się przez to właściwość zapewniającą, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

3) poufność – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

4) integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej jak i przypadkowej.

5) dostępność – gwarantuje, że osoby, które są upoważnione i którym informacje są potrzebne, mają do nich dostęp w odpowiednim miejscu i czasie.

3. Za przestrzeganie zasad ochrony i bezpieczeństwa informacji odpowiedzialni są upoważnieni użytkownicy.

§ 4

Realizację zamierzeń określonych w § 3 powinny zagwarantować następujące założenia:

1) Wdrożenie procedur określających postępowanie osób dopuszczonych do przetwarzania informacji oraz ich odpowiedzialność za ochronę danych.
2) Przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony informacji.
3) Przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory),
4) Podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń,
5) Okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych,
6) Opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii.
7) Okresowe aktualizowanie Polityki Bezpieczeństwa Informacji.
8) Identyfikacja zagrożeń i analiza ryzyka

Rozdział II
OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ INFORMACJI

§ 5

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.

§ 6

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są informacje 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,

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,

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 informacji - 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 bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane,

13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych, itp.).

§ 7

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

Rozdział III

PRZEDSIĘWZIĘCIAZABEZPIECZAJĄCE PRZED NARUSZENIEM OCHRONY DANYCH

§ 8

1. Każdy użytkownik – przed dopuszczeniem do przetwarzania informacji podlega przeszkoleniu z przepisów w zakresie ochrony informacji oraz wynikających z nich zadań
   i obowiązków.
2. Wszyscy użytkownicy podlegają okresowym szkoleniom.

§ 9

Za organizację szkoleń odpowiedzialny jest Administrator Bezpieczeństwa Informacji.

§ 10

1. Dla zapewnienia bezpieczeństwa danych i informacji zastosowano następujące środki organizacyjne:

1) Dostęp do danych osobowych mogą mieć tylko i wyłącznie pracownicy posiadający pisemne, imienne upoważnienia podpisane przez Administratora Danych.
2) Każdy z pracowników powinien zachować szczególną ostrożność przy przetwarzaniu, przenoszeniu wszelkich.
3) Należy chronić dane przed wszelkim dostępem do nich osób nieupoważnionych.
4) Pomieszczenia w których są przetwarzane dane osobowe muszą być zamykane na klucz.
5) Dostęp do kluczy posiadają tylko upoważnieni pracownicy.
6) Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy. W wypadku gdy jest wymagany poza godzinami pracy – możliwy jest tylko na podstawie zezwolenia Administratora Bezpieczeństwa Informacji.
7) Dostęp do pomieszczeń w których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy.
8) W przypadku pomieszczeń do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności.
9) Szafy w których przechowywane są dane muszą być zamykane na klucz.
10) Klucze do tych szaf posiadają tylko upoważnieni pracownicy.
11) Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych a następnie powinny być zamykane.
12) Dane w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych a następnie muszą być chowane do szaf.

2. Dla zapewnienia bezpieczeństwa danych i informacji zastosowano następujące środki techniczne:

1) Dostęp do komputerów na których są przetwarzane dane mają tylko upoważnieni pracownicy.
2) Monitory komputerów na których przetwarzane są dane są tak ustawione aby osoby nieupoważnione nie miały wglądu w dane.
3) Po zakończeniu pracy komputery przenośne (np. typu notebook) zawierające dane osobowe powinny być zabezpieczone w zamykanych na klucz szafach.
4) W wypadku potrzeby wyniesienia komputera przenośnego (np. typu notebook) zawierającego dane osobowe, lub inne informacje chronione, komputer taki musi być odpowiednio dodatkowo zabezpieczony, a dane zaszyfrowane.
5) Nie należy udostępniać osobom nieupoważnionym tych komputerów.

6) W przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności.
7) Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie) aby nie zostały na nich dane osobowe.
8) W wypadku niemożliwości skasowania danych z nośnika (płyta CD-ROM) należy taką płytę zniszczyć fizycznie.
9) W przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków.
10) Niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną.
11) Sieć komputerowa powinna jest zabezpieczona przed wszelkim dostępem z zewnątrz.
12) Błędne lub nieaktualne wydruki i wersje papierowe zawierające dane osobowe lub inne informacje chronione niszczone są za pomocą niszczarki lub w inny mechaniczny sposób uniemożliwiający powtórne ich odtworzenie.

Rozdział IV

DOSTĘP DO INFORMACJI i DANYCH OSOBOWYCH

§ 11

1. Przetwarzanie, w tym udostępnianie danych osobowych jest prawnie dopuszczalne, jeżeli jest niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego
   z przepisu prawa.
2. W przypadku udostępnienia danych osobowych w celach innych niż włączenie do zbioru, administrator danych udostępnia posiadane informacje osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
3. Dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
4. Podmiot występujący o udostępnienie informacji powinien wskazać podstawę prawną upoważniającą go do otrzymania tych danych albo uzasadnioną potrzebę żądania ich udostępnienia. Tylko w takiej sytuacji można dokonać oceny, czy w określonym przypadku udostępnienie danych jest prawnie dopuszczalne i czy nie będzie ono stanowić naruszenia zasad ochrony informacji.
5. Przetwarzanie, w tym udostępnianie informacji w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której

dane dotyczą, oraz następuje w celu badań naukowych, dydaktycznych, historycznych

oraz statystycznych, z zachowaniem przepisów art. 23 i 25 ustawy o ochronie danych osobowych.

6. Udostępnienie informacji może nastąpić jedynie za zgodą Administratora Danych lub osoby przez niego upoważnionej.

§ 12

1. Szczegółowy wykaz zbiorów danych osobowych ze wskazaniem programów zastosowanych do ich przetwarzania zawiera załącznik nr 4.
2. Za prowadzenie i nadzór wykazu odpowiada ABI.

Rozdział V

KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA INFORMACJI

§ 13

1. Administrator Danych lub osoba przez niego wyznaczona, którą jest ABI sprawuje nadzór nad przestrzeganiem zasad ochrony informacji wynikających z aktualnie obowiązujących przepisów prawa w tym zakresie oraz zasad ustanowionych w niniejszym dokumencie.
2. ABI sporządza plany kontroli zatwierdzone przez Administratora Danych i zgodnie z nimi przeprowadza kontrole oraz dokonuje ocen stanu bezpieczeństwa informacji.
3. Plan kontroli przedstawiony jest w załączniku nr 7

Rozdział VI

POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH

§ 14

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.) każda osoba zatrudniona przy przetwarzaniu danych jest obowiązana niezwłocznie powiadomić o tym fakcie ABI.

§ 15

W razie niemożliwości zawiadomienia ABI lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego.

§ 16

Do czasu przybycia na miejsce naruszenia ochrony danych osobowych ABI lub upoważnionej przez niego osoby, 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) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ABI lub osoby upoważnionej.

§ 17

Po przybyciu na miejsce naruszenia ochrony informacji, ABI lub osoba go zastępująca:

1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy ,

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 placówki.

§ 18

ABI dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, 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.

§ 19

1. Raport ABI niezwłocznie przekazuje Administratorowi Danych, a w przypadku jego nieobecności osobie uprawnionej.

2. Raport z naruszenia ochrony danych opisuje załącznik nr 8 do niniejszej Polityki.

§ 20

Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator Bezpieczeństwa Informacji zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

§ 21

Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Administratora Danych, ABI, Informatyka oraz osób wyznaczonych przez Administratora Danych.

§ 22

Analiza 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 VII

POSTANOWIENIA KOŃCOWE

§ 23

Wobec osoby, która w przypadku naruszenia środków bezpieczeństwa danych 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 lub porządkowe.

§ 24

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

§ 25

Polityka jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym w żadnej formie.

§ 26

1. Użytkownicy są zobowiązani zapoznać się z treścią Polityki
2. Użytkownik zobowiązany jest złożyć oświadczenie o tym, iż został zaznajomiony
   z przepisami ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych, z niniejszą Polityką, a także zobowiązać się do ich przestrzegania.
3. Wzór oświadczenia potwierdzającego zaznajomienie użytkownika z przepisami w zakresie ochrony informacji oraz z dokumentacją obowiązującą u Administratora Danych, a także
   o zobowiązaniu się do ich przestrzegania, stanowi załącznik nr 5 do niniejszej Polityki.

4. Oświadczenia przechowywane są w aktach osobowych.

§ 27

1. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie aktualnie obowiązujące przepisy prawa w zakresie ochrony informacji.
2. Użytkownicy zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych postanowień zawartych w niniejszej Polityce. W wypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach obowiązujących u Administratora Danych, użytkownicy mają obowiązek stosowania unormowań dalej idących, których stosowanie zapewni wyższy poziom ochrony informacji.

……..

(podpis Administratora Danych)

Załącznik nr 1

WYZNACZENIE ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

Obowiązki Administratora Bezpieczeństwa Informacji (ABI), do zadań którego należy:

- nadzór przestrzegania zasad ochrony przetwarzanych danych według procedur opisanych w niniejszej Polityce,
- nadzór środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną,

przetwarzaniem z naruszeniem przepisów, oraz zmianą, utratą, uszkodzeniem, lub zniszczeniem,

- przeprowadzanie kontroli w zakresie określonym regulacjami wewnętrznymi Administratora Danych,

pełni …….

……..

(podpis Administratora Danych)

……..

(podpis Administratora Bezpieczeństwa Informacji)

Załącznik nr 2

WYZNACZENIE ADMINISTRATORA SYSTEMU INFORMATYCZNEGO (INFORMATYKA)

Obowiązki Administratora Systemu Informatycznego (Informatyka), który dba o:

- prawidłowe funkcjonowanie sprzętu, oprogramowania i jego konserwację,
- techniczno-organizacyjną obsługę systemu teleinformatycznego,
- należyte wywiązywanie się z obowiązków wynikających z Instrukcji zarządzania systemem informatycznym

pełni na podstawie stosownej umowy ……

…….. ……..

(podpis Administratora Danych) (podpis Informatyka)

Załącznik nr 3

OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH

1. Przetwarzanie danych z użyciem stacjonarnego sprzętu komputerowego i kartotek odbywa się wyłącznie w obszarze przetwarzania danych.
2. Obszarem przetwarzania danych są pomieszczenia na I piętrze budynku
   przy ul. Kościuszki 30, 39-400 Tarnobrzeg, w których przetwarzane są dane osobowe,
3. Obszarem przetwarzania danych nie są pomieszczenia socjalne i ogólnie dostępne.
4. Przetwarzanie danych jest zabronione, jeśli nie są zapewnione warunki ochrony danych osobowych określone w niniejszej Polityce.

Załącznik nr 4
do Polityki bezpieczeństwa danych osobowych

WYKAZ ZBIORÓW DANYCH OSOBOWYCH
ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO ICH PRZETWARZANIA

L.p.	**NAZWA ZBIORU**	**NAZWA PROGRAMU**
1.	OBSŁUGA FINANSOWO - KSIĘGOWA PLACÓWEK OŚWIATOWYCH	
2.	ARCHIWUM	
3.	DOSKONALENIE ZAWODOWE	
4.	KOMISJA SOCJALNA	
5.	ZAMÓWIENIA PUBLICZNE	
6.	REJESTR SKARG I WNIOSKÓW	
7.	REJESTR WNIOSKÓW O DOSTĘP DO INFORMACJI PUBLICZNEJ	

Załącznik nr 5

…….
(imię i nazwisko)

……
(miejscowość, data)

OŚWIADCZENIE

Oświadczam, że zostałem/zostałam zapoznany/zapoznana* z:*

– Polityką bezpieczeństwa danych osobowych,

– Instrukcją zarządzania systemem informatycznym służącym do przetwarzania informacji w tym danych osobowych.

Jednocześnie oświadczam, że zobowiązuje, się przestrzegać zasad ochrony danych osobowych podczas wykonywania obowiązków służbowych, w tym zobowiązuję się do:

– dołożenia wszelkich starań przy wykonywaniu powierzonych mi obowiązków w celu ochrony danych osobowych,

– przetwarzania danych osobowych zgodnie z obowiązującymi w tym zakresie przepisami prawa i regulacjami wewnętrznymi Szkoły,

– do zabezpieczenia przetwarzanych danych osobowych przed ich:

a) udostępnieniem osobom nieupoważnionym,

b) zabraniem przez osobę nieuprawnioną,

c) przetwarzaniem z naruszeniem przepisów prawa,

d) nieuprawnioną zmianą lub zniszczeniem,

e) utratą,

f) uszkodzeniem,

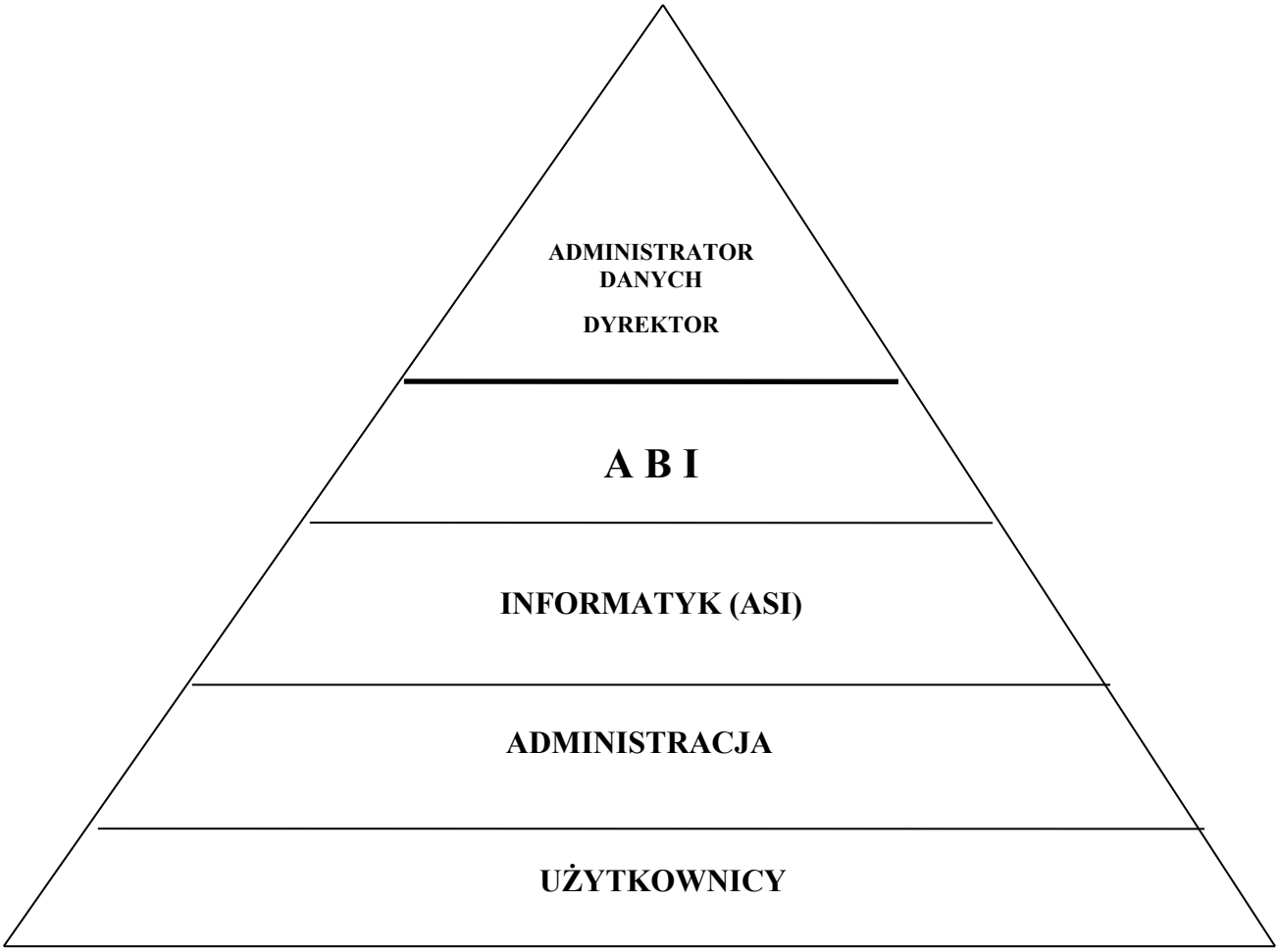
– do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, również po ustaniu zatrudnienia.

…….
(podpis osoby składającej oświadczenie)

* niepotrzebne skreślić

Załącznik nr 6

ORGANIZACJA NADZORU OCHRONY DANYCH OSOBOWYCH



Załącznik nr 7

REGULAMIN I HARMONOGRAM KONTROLI MECHANIZMÓW OCHRONY DANYCH OSOBOWYCH

PODSTAWA PRAWNA

Polityka bezpieczeństwa ochrony danych osobowych opracowana zgodnie z aktualnymi wymogami przepisów prawa z zakresu ochrony danych osobowych, ze szczególnym uwzględnieniem Ustawy o ochronie danych osobowych (Dz.U. 1997 Nr 133 poz. 883)

1. Plan regulaminu kontroli wewnętrznej obejmuje następujące zagadnienia:

- funkcjonowanie zabezpieczeń systemowych

- prawidłowość funkcjonowania mechanizmów dostępu do zbioru danych

- funkcjonowanie zastosowanych zabezpieczeń fizycznych,

- zasady przechowywania kartotek,

- zasady i sposoby likwidacji oraz archiwizowania zbiorów archiwalnych

- realizacja procedur wdrożonych przez Administratora Danych w zakresie ochrony danych osobowych,

2. Zagadnienia, czynności kontrolno-oceniające ujęte są w harmonogramie ich przeprowadzania, ze wskazaniem osób je wykonujących.

3. Dodatkowe czynności kontrolne potwierdzone są w zakresie zadań, kompetencji i odpowiedzialności tych pracowników, którzy takie uprawnienia z relacji zajmowanych stanowisk posiadają.

4. Za zorganizowanie i prawidłowe działanie kontroli wewnętrznej, a także za należyte wykorzystanie wyników kontroli odpowiedzialny jest Administrator bezpieczeństwa informacji

5. Z kontroli wewnętrznej kontrolujący sporządza pisemną notatkę. Z wynikami kontroli zapoznaje kontrolowane strony i Administratora danych

L.P.	**ZAGADNIENIA – ZAKRES KONTROLI**	**OSOBY ODPOWIEDZIALNE**	**TERMIN – CZĘSTOTLIWOŚĆ KONTROLI**	**OSOBY KONTROLUJĄCE**	**UWAGI I WNIOSKI**

1.	Analiza Polityki Bezpieczeństwa Informacji oraz Instrukcji zarządzania systemem informatycznym. Sprawdzenie jej zgodności z aktualnymi przepisami.	ABI, Informatyk	Zgodnie z bieżącą sytuacją , nie rzadziej jak raz na rok.	ABI, Informatyk	
2.	Sprawdzenie zakresu, rodzaju zbieranych danych, celów w jakich są zbierane i adekwatności.	Kierownicy zespołów		ABI	
3.	Sprawdzenie treści klauzul informacyjnych i klauzul zgody na przetwarzanie danych.			ABI	
4.	Weryfikacja zbiorów danych osobowych i ich zgłoszeń do GIODO	ABI		ABI	
5.	Sprawdzenie umów z zewnętrznymi firmami pod kątem możliwości powierzenia lub dostępu do danych		Każdorazowo przy zawieraniu umów		
6.	Weryfikacja ewidencji osób upoważnionych do przetwarzania danych osobowych	ABI		ABI	
7.	Ustalenie jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane			Informatyk	
8.	sprawdzenie skuteczności zastosowanych środków technicznych (antywirusy, UPS, hasła itp.)	Użytkownicy przetwarzający dane w systemie informatycznym	W zależności od potrzeby, nie rzadziej niż raz na kwartał.	Informatyk	
9.	Badanie mechanizmów logowania i uwierzytelniania użytkownika	Użytkownicy przetwarzający dane w systemie		Informatyk	

		informatycznym			
10.	Sprawdzenie technicznych środków bezpieczeństwa (drzwi, monitoring, p-poż, gospodarka kluczami itp.)		Raz w roku	ABI	
11.	Sprawdzenie urządzeń przenośnych i kryptograficznych metod ochrony przetwarzanych na nich danych	Użytkownicy przetwarzający dane na urządzeniach przenośnych, które mogą być wynoszone poza obszar przetwarzania	Raz na pół roku	Informatyk	
12.	analiza harmonogramu i zakresu szkoleń z zakresu ochrony danych osobowych w celu oceny, czy skutecznie wpływają na podwyższenie świadomości osób uczestniczących w przetwarzaniu danych	Pracownicy i nowi pracownicy	Bieżące rozwiązywanie problemów, szkolenia stanowiskowe, instruktaże dla nowych pracowników	ABI, Informatyk	
13	Sprawdzić kopie zapasowe; okresy ich tworzenia, oznakowanie, przechowywanie	Osoby upoważnione do tworzenia zapasowych kopii doraźnych.	Zgodnie z częstotliwością określoną przez Informatyka	Informatyk	
14.	Inwentaryzacja oprogramowania, sprawdzenie jego zgodności z licencjami i prawami autorskimi	Kierownicy zespołów		Informatyk	
15.	Upoważnienia osób do przetwarzania danych oraz aktualność ewidencji osób			ABI	

	upoważnionych				
16.	Obowiązek informacyjny – klauzule zgody i informacyjne			ABI	
17.	Zasady udostępniania i powierzania danych				
18.	Zasady postępowania w sytuacjach naruszenia ochrony danych osobowych				

Załącznik nr 8

RAPORT Z NARUSZENIA OCHRONY DANYCH

1. Data ……. Godzina ……

2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe,):

……..

……..

……..

3. Lokalizacja zdarzenia (nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):

……

……

4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:

……

……

5. Podjęte działania:

……

6. Wstępna ocena przyczyn wystąpienia naruszenia:

…….

7. Postępowanie wyjaśniające i naprawcze:

…….

……. …….(podpis pracownika) (data i podpis ABI)

Załącznik Nr 2 do Zarządzenia Nr 16/2013

Dyrektora Miejskiego Oświatowego Zespołu Ekonomicznego
w Tarnobrzegu z dnia 22.11.2013

I N S T R U K C J A
ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH MIEJSKIEGO OŚWIATOWEGO ZESPOŁU EKONOMICZNEGO W TARNOBRZEGU

Spis treści

POSTANOWIENIA OGÓLNE

§ 1

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „Instrukcją”, określa sposób zarządzania systemem

informatycznym służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji, a także zasady i tryb postępowania Administratora Danych oraz osób przez niego upoważnionych przy przetwarzaniu danych osobowych.

2. Instrukcja została opracowana zgodnie z wymogami określonymi w § 5 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 do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024)

§ 2

Instrukcja określa procedury i warunki zarządzania systemem informatycznym oraz kartotekami, zapewniające ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

§ 3

1. Ilekroć w Instrukcji jest mowa o:
    1) Zbiorze danych – rozumie się przez to każdy posiadający strukturę zestaw danych
    o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od twego, 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.

    3) Systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych

    4) Kartotece – rozumie się przez to zewidencjonowany, usystematyzowany zbiór wykazów, skoroszytów, wydruków komputerowych i innej dokumentacji gromadzonej
    w formie papierowej, zawierającej dane osobowe

    5) Administratorze Danych – rozumie się przez to Miejski Oświatowy Zespół Ekonomiczny w Tarnobrzegu, reprezentowany przez Dyrektora.

6) Administratorze Bezpieczeństwa Informacji, zwanego dalej „ABI” – rozumie się przez to osobę nadzorującą przestrzeganie zasad ochrony przetwarzanych danych osobowych i informacji prawem chronionych. Nadzoruje on stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz zmianą, utratą, uszkodzeniem, lub zniszczeniem, a także przeprowadza kontrole w zakresie określonym regulacjami wewnętrznymi Administratora Danych.

Administratora bezpieczeństwa informacji wyznacza Administrator danych, chyba że sam wykonuje te czynności.
Wyznaczenie ABI opisuje załącznik nr 1 do niniejszej Polityki bezpieczeństwa informacji i ochrony danych osobowych.

6) Osobie odpowiedzialnej za prawidłowe funkcjonowanie sprzętu, oprogramowania i jego konserwację – rozumie się prze to wyznaczonego przez Administratora Danych informatyka odpowiedzialnego za powyższe zadania, zwanego dalej „Informatykiem", który pełni rolę Administratora Systemu Informatycznego.

7) Komórce organizacyjnej – rozumie się przez to każdą wydzieloną organizacyjnie i funkcjonalnie komórkę wewnętrzną, zgodnie z regulaminem organizacyjnym

8) Użytkowniku – rozumie się przez to osobę wyznaczoną przez Administratora Danych do przetwarzania danych osobowych w systemie informatycznym oraz kartotekach

9) Pomieszczeniach – rozumie się przez to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego lub gromadzone w kartotekach

§ 4

1. Podstawowym celem zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych jest zapewnienie jak najwyższego standardu bezpieczeństwa tych danych. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania, charakteru poufnego wraz z zachowaniem ich integralności oraz integralności systemu informatycznego.

2. W celu zwiększenia efektywności ochrony danych osobowych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.

3. Zastosowane zabezpieczenia maja służyć osiągnięciu poniższych celów i zapewnić:
1) poufność danych – rozumianą jako właściwość zapewniającą, że dane nie
2) są udostępniane nieupoważnionym osobom,
3) integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
4) rozliczalność danych – rozumiana jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
5) integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

4. Za przestrzeganie zasad ochrony i bezpieczeństwa danych odpowiedzialni są użytkownicy.

§ 5

1. Uwzględniając kategorie przetwarzanych danych oraz zagrożenia wprowadza się wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym.

2. Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną.

§ 6

Realizację zamierzeń określonych w § 4 powinny zagwarantować następujące założenia:

1) wdrożenie procedur określających postępowanie osób dopuszczonych do przetwarzania danych osobowych oraz ich odpowiedzialność za ochronę tych danych.
2) Przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych
3) Przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory) oraz zapewniających dostęp użytkowników do różnych poziomów zbiorów danych osobowych – stosownie do indywidualnego zakresu upoważnienia,
4) Podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń,
5) Okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych,
6) Opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii,
7) Śledzenie osiągnięć w dziedzinie zabezpieczenia systemów informatycznych. Wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemem informatycznym, które będą służyły wzmocnieniu bezpieczeństwa danych osobowych.

PRZYDZIAŁ UPRAWNIEŃ I IDENTYFIKATORÓW

§ 7

1. Każdy użytkownik dopuszczony do przetwarzania danych osobowych posiada stosowne upoważnienie. Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr. 1 do Instrukcji.

2. Każdy użytkownik posiada indywidualny identyfikator umożliwiający logowanie do tych aplikacji, z którymi może pracować.

3. Identyfikator umożliwia wykonanie czynności zgodnie z zakresem powierzonych obowiązków, które wyznaczają poziom uprawnień.

4. Informatyk zobowiązany jest do prowadzenia ewidencji przyznanych poszczególnym użytkownikom uprawnień związanych z dostępem do zbiorów danych oraz dokonywaniem zmian w zakresie przyznanych uprawnień.

§ 8.

Każdy użytkownik systemu informatycznego przetwarzającego dane osobowe powinien posiadać umiejętność bezpiecznej obsługi komputera i dobrą znajomość oprogramowania systemowego i operacyjnego, z którego będzie korzystał.

§ 9.

1. Każdy użytkownik – przed dopuszczeniem do obsługi systemu informatycznego, w którym przetwarzane są dane osobowe – podlega przeszkoleniu w zakresie:
1) obsługi komputera, oprogramowania systemowego oraz oprogramowania do obsługi aplikacji, którą będzie wykorzystywał,
2) przepisów o ochronie danych osobowych oraz wynikających z nich zadań i obowiązków.

2. Wszyscy użytkownicy podlegają okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (wymiana sprzętu, oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji.

§ 10

Za organizację szkoleń, o których mowa w § 9 odpowiedzialny jest Administrator Bezpieczeństwa Informacji.

§ 11.

Do uwierzytelnienia użytkowników w systemie używa się haseł lub innych metod zapewniających weryfikację tożsamości użytkownika.

§ 12.

Każdy użytkownik zobowiązany jest do zachowania w tajemnicy własnych haseł, także po upływie ich ważności.

§ 13.

1. Identyfikatory dla użytkowników upoważnionych do przetwarzania danych osobowych w systemie informatycznym, niezbędne do logowania się do określonej aplikacji, ustala i przydziela informatyk lub inna osoba upoważniona przez Administratora Danych.

2. Identyfikator użytkownika nie podlega zmianie.

3. Identyfikator użytkownika podlega rejestracji w systemie informatycznym.

§ 14.

1. Pierwsze hasło dla użytkownika ustala informatyk przy wprowadzeniu identyfikatora użytkownika do systemu.

2. Hasła muszą odpowiadać następującym wymogom:

1) hasła składają się przynajmniej z 8 znaków, i powinny zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
2) nie mogą być zapisywane w systemie w postaci jawnej,
3) nie mogą być w nich używane imiona, nazwiska, przezwiska, inicjały i inne kombinacje znaków mogących doprowadzić do łatwego rozszyfrowania haseł przez osoby nieupoważnione,
4) nie mogą być w nich stosowane znaki następujące po sobie na klawiaturze bądź też same litery czy cyfry.

§ 15.

1. Po otrzymaniu pierwszego hasła użytkownik zobowiązany jest zalogować się do systemu i powinien zmienić hasło. Przy wpisywaniu hasło nie może być wyświetlane na ekranie.

2. Hasło zmieniane jest nie rzadziej niż co 30 dni. Za systematyczną, terminową zmianę hasła odpowiada użytkownik .

§ 16.

Hasło podlega natychmiastowej zmianie w przypadku podejrzenia jego odkrycia przez nieupoważnioną osobę.

§ 17.

1. Hasła nie mogą być nigdzie zapisywane, z wyjątkiem haseł informatyka, które przechowywane są w opieczętowanych kopertach, w miejscu wyznaczonym przez Administratora Bezpieczeństwa Informacji.

2. Tryb przechowywania i udostępniania haseł Informatyka określa załącznik nr 2 do Instrukcji.

REJESTROWANIE I WYREJESTROWYWANIE UŻYTKOWNIKÓW

§ 18

1. Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi Administrator Bezpieczeństwa Informacji lub osoba wyznaczona przez Administratora Danych. Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych stanowi załącznik nr 3 do Instrukcji.

2. Ewidencja zawiera:
1) imię i nazwisko użytkownika,
2) datę nadania i ustania upoważnienia
3) zakres upoważnienia
4) identyfikator użytkownika

3. Ewidencja użytkowników może być prowadzona w systemie informatycznym

§ 19

Zmiany dotyczące użytkownika, takie jak:
1) zmiana imienia lub nazwiska,
2) zmiana zakresu upoważnienia,

podlegają niezwłocznemu odnotowaniu w ewidencji, o której mowa w § 18 Instrukcji.

§ 20

1. Zmiany dotyczące użytkownika, takie jak:
1) rozwiązanie umowy,
2) utrata upoważnienia do przetwarzania danych osobowych
3) zmiana zakresu obowiązków służbowych skutkująca ustaniem upoważnienia,

powodują wyrejestrowanie użytkownika przez Informatyka w trybie natychmiastowym z ewidencji, o której mowa w § 18 Instrukcji, zablokowanie identyfikatora oraz unieważnienie hasła tego użytkownika.

2. Kierownicy komórek organizacyjnych odpowiadają za natychmiastowe zgłoszenie do Informatyka użytkowników, którzy utracili uprawnienia do dostępu do danych osobowych, celem zablokowania im dostępu do systemu informatycznego poprzez zablokowanie identyfikatora i wyrejestrowanie z ewidencji użytkowników, o której mowa w § 18 Instrukcji.

3. Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi

PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

§ 21

Przed przystąpieniem do pracy z systemem informatycznym lub kartotekami, użytkownik zobowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz dokonać oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie poufności danych osobowych.

§ 22

W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie systemu, użytkownik obowiązany jest postępować zgodnie z zasadami określonymi w Polityce bezpieczeństwa.

§ 23

1. Rozpoczynając pracę na komputerze użytkownik loguje się do systemu informatycznego.
2. Użytkownik wprowadza identyfikator i dokonuje uwierzytelnienia.
3. Jeśli system to umożliwia, po przekroczeniu ustalonej liczby prób logowania system blokuje dostęp do systemu informatycznego na poziomie danego użytkownika.
4. Informatyk ustala przyczyny zablokowania systemu oraz w zależności od zaistniałej sytuacji podejmuje odpowiednie działania. O zaistniałym incydencie powiadamia Administratora Bezpieczeństwa Informacji lub osobę przez niego wyznaczoną.

§ 24

Przed opuszczeniem stanowiska pracy, użytkownik obowiązany jest:
1) wylogować się z systemu informatycznego lub
2) poczekać, aż zaktywizuje się blokowany hasłem wygaszasz ekranu.

§ 25

Kończąc pracę należy:
1) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
2) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe, przed dostępem osób nieuprawnionych.

PROCEDURY TWORZENIA KOPII ZAPASOWYCH

§ 26

1. Zbiory danych osobowych oraz programy i narzędzia programowe służące do ich przetwarzania, zapisywane na nośnikach zewnętrznych tworzące kopie zapasowe kolejnych okresów, powinny być odpowiednio oznakowane i przechowywane w wyznaczonych, odpowiednio zabezpieczonych pomieszczeniach.
2. Kopie zapasowe określone w ust. 1 niniejszego paragrafu powinny być sporządzane regularnie w okresach wyznaczonych przez Administratora Danych.
3. Za prawidłowe sporządzanie kopii zapasowych, ich oznakowanie i przechowywanie, odpowiedzialny jest Informatyk.
4. Odpowiada on także za sprawdzanie poprawności wykonania kopii zapasowych na nośnik zewnętrzny.

5. Kopie zapasowe powinny być przechowywane w pomieszczeniu odrębnym od pomieszczeń, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.

§ 27

1. Użytkownicy obowiązani są przestrzegać terminów tworzenia doraźnych kopii zapasowych o ile zostali do tego upoważnieni przez Informatyka.
2. Użytkownicy określeni w ust. 1 są odpowiedzialni za prawidłowe sporządzanie kopii zapasowych, ich oznakowanie i przechowywanie.

§ 28

1. Kopie zapasowe, które uległy uszkodzeniu lub ustała ich użyteczność podlegają natychmiastowemu zniszczeniu z zachowaniem procedur określonych niniejszą Instrukcją.
2. Zniszczenia kopii zapasowych na nośnikach magnetycznych i optycznych dokonuje Informatyk.
3. Z nośników magnetycznych i optycznych wielokrotnego użytku dane należy usunąć w sposób uniemożliwiający ich odczytanie, a w przypadku gdy usunięcie danych nie jest możliwe, nośniki podlegają zniszczeniu w stopniu uniemożliwiającym odzyskanie danych.
4. Dane zawarte na nośnikach optycznych jednokrotnego użytku, należy usuwać poprzez całkowite zniszczenie nośnika.

PRZETWARZANIE DANYCH OSOBOWYCH

§ 29

1. Dane osobowe przetwarzane są w kartotekach oraz w komputerach do tego przeznaczonych (serwerach, stacjach roboczych) zlokalizowanych w obszarach przetwarzania danych osobowych.
2. W przypadku przekazywania urządzeń lub nośników zawierających dane osobowe, zwłaszcza tzw. „wrażliwe”, o których mowa w art. 27 ust 1. ustawy o ochronie danych osobowych, poza obszar przetwarzania danych osobowych, zabezpiecza się je w sposób zapewniający poufność i integralność tych danych, przez co rozumie się:

1) ograniczenie dostępu do danych osobowych hasłem zabezpieczającym dane przed osobami nieupoważnionymi, lub
2) stosowanie metod kryptograficznych, lub
3) stosowanie odpowiednich zabezpieczeń fizycznych, lub
4) w zależności od stopnia zagrożenia zalecane jest stosowanie kombinacji wyżej wymienionych zabezpieczeń

3. Dane osobowe zapisywane na nośnikach zewnętrznych tworzące kopie zapasowe kolejnych okresów, powinny być przechowywane w wyznaczonych, odpowiednio zabezpieczonych pomieszczeniach.
4. Kartoteki powinny być przechowywane w szafach, znajdujących się w wyznaczonych, odpowiednio zabezpieczonych pomieszczeniach.
5. Wydruki robocze, błędne lub zdezaktualizowane powinny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowanie.
6. Szczegółowy opis obszaru przetwarzania danych osobowych oraz środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności danych osobowych określony jest w Polityce bezpieczeństwa.

§ 30

1. Kartoteka przekazywana jest do archiwum zgodnie z procedurami archiwizacji dokumentów.
2. Likwidacji zbiorów archiwalnych dokonuje się przy użyciu niszczarki do papieru lub
3. w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowanie.

§ 31

Decyzję o likwidacji zbiorów danych osobowych, przetwarzanych w kartotekach oraz systemach informatycznych, podejmuje Administrator Danych na wniosek Administratora Bezpieczeństwa Informacji.

§ 32

Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów danych osobowych, Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona sporządza protokół, w którym zamieszcza następujące informacje:

1) datę dokonania likwidacji
2) przedmiot likwidacji (nośniki, kartoteka)
3) przedział czasowy likwidowanych zbiorów danych osobowych
4) podpisy osób dokonujących i obecnych przy likwidacji zbiorów danych osobowych

ZABEZPIECZENIE SYSTEMU INFORMATYCZNEGO

§ 33

System informatyczny zabezpiecza się przed:

1) działaniem, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
2) utratą danych spowodowaną:
a) działaniem nieautoryzowanego oprogramowania
b) awarią zasilania lub zakłóceniami w sieci zasilającej

§ 34

1. Informatyk odpowiada za niezwłoczne instalowanie na sprzęcie najnowszych wersji oprogramowania zabezpieczającego system informatyczny.

2. Nowe wersje oprogramowania instaluje wyłącznie Informatyk niezwłocznie po ich otrzymaniu lub osoba przez niego upoważniona

3. Okresowych kontroli w zakresie instalowania najnowszych wersji oprogramowania zabezpieczającego system informatyczny dokonuje Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona.

§ 35

1. Na serwerach i stacjach roboczych używanych przez Administratora Danych powinno instalować się przynajmniej jeden program antywirusowy.

2. Program antywirusowy należy instalować również na komputerach przenośnych.

§ 36

W komputerach przenośnych zawierających dane osobowe stosuje się środki ochrony kryptograficznej wobec przetwarzania danych osobowych.

§ 37

1. Kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i optycznych służących zarówno do przetwarzania danych osobowych w systemie informatycznych jak i do celów instalacyjnych

2. Na serwerach, w miarę możliwości technicznych, oprogramowanie antywirusowe powinno być aktywne cały czas.

3. Na stacjach roboczych oprogramowanie antywirusowe powinno być aktywne cały czas i powinno dokonywać sprawdzenia każdego otwieranego lub uruchomianego pliku.

§ 38

Użytkownicy są zobowiązani do dokonywania kontroli antywirusowej wszystkich nośników magnetycznych lub optycznych przychodzących z zewnątrz oraz okresowo nośników własnych.

§ 39

1. W razie stwierdzenia zainfekowania systemu, użytkownik obowiązany jest poinformować niezwłocznie o tym Informatyka.

2. Informatyk usuwa wirusa, jeśli automatycznie nie dokonał tego program antywirusowy oraz informuje Administratora Bezpieczeństwa Informacji lub osobę przez niego upoważnioną o dokonanych czynnościach i rodzaju wirusa.

§ 40

W razie niemożności usunięcia wirusa, Informatyk za zgodą Administratora Bezpieczeństwa Informacji, korzysta z usług zewnętrznych w tej dziedzinie.

§ 41

1. W sytuacji korzystania z usług zewnętrznych specjalistów, należy podjąć działania uniemożliwiające tym osobom dostęp do danych osobowych.

2. Prace określone w ust. 1 są wykonywanie pod nadzorem Informatyka lub upoważnionego użytkownika i w miarę możliwości bez dostępu do danych osobowych.

§ 42

1. Informatyk jest odpowiedzialny za kontrolę antywirusową serwerów i zasobów sieciowych.
2. Użytkownicy są odpowiedzialni za kontrolę antywirusową na dyskach lokalnych i używanych nośnikach danych.

§ 43

Po usunięciu wirusa Informatyk sprawdza zainfekowany system informatyczny oraz przywraca go do pełnej sprawności i funkcjonalności.

§ 44

1. Przy przetwarzaniu danych osobowych zakwalifikowanych do poziomu bezpieczeństwa wysokiego system informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
2. W przypadku zastosowania logicznych zabezpieczeń, o których mowa w ust. 1, obejmują one:
1) kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną,
2) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego
3. Wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej stosuje się środki ochrony kryptograficznej.

§ 45

Informatyk prowadzi wykaz przypadków zainfekowania komputerów i nośników wykorzystywanych do przetwarzania danych osobowych w systemie oraz przechowuje kopie raportów.

§ 46

Procedura wyrażona w niniejszym rozdziale ma zastosowanie także do przypadków awarii systemu spowodowanych błędem programu bądź użytkownika.

WYMAGANIA DOTYCZĄCE SPRZĘTU I OPROGRAMOWANIA

§ 47

1. Sprzęt obsługujący zbiór danych osobowych składa się z komputerów stacjonarnych klasy PC.
2. Komputery przenośne mogą być używane do przetwarzania danych osobowych
3. po odpowiednim ich zabezpieczeniu.
4. Użytkownik korzystający z komputera przenośnego jest zobowiązany do zachowania szczególnej ostrożności podczas transportu komputera oraz nie może udostępnić komputera osobom nieupoważnionym

§ 48

1. Sieć komputerowa służąca do przetwarzania danych osobowych powinna mieć zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu komputerowego.
2. Sieć komputerowa powinna być podłączona do zasilania zapasowego (zasilanie dwustronne, agregat prądotwórczy lub UPS). Oprogramowanie powinno zapewnić bezpieczne wyłączenie systemu informatycznego, po dokonaniu operacji zamknięcia w pracujących aplikacjach i oprogramowaniu systemowym.
3. Serwer sieci powinien być zasilany przez UPS o odpowiednich parametrach, pozwalających na podtrzymanie napięcia oraz na wykonanie bezpiecznego wyłączenia serwera, tak aby przed zanikiem zasilania zostały prawidłowo zakończone operacje rozpoczęte na zbiorze danych osobowych.
4. Zasilaniem awaryjnym powinna być zabezpieczona co najmniej jedna stacja robocza.

§ 49

1. Prawidłowe zasilanie energetyczne sieci komputerowej sprawdza Informatyk.
2. Infrastruktura techniczna związana z siecią komputerową i jej zasilaniem (rozdzielnie elektryczne, skrzynki z bezpiecznikami) powinna być zabezpieczona przed dostępem osób nieupoważnionych.
3. Wszystkie urządzenia w sieci komputerowej (pozostałe stacje robocze, drukarki, modemy itd.) powinny być w miarę możliwości technicznych włączone do wydzielonej sieci energetycznej, zapewniającej odpowiednie uziemienie i zabezpieczenie przed przepięciami.

4. Gniazda zasilania sieci komputerowej powinny być odpowiednio oznakowane, zabezpieczone przed włączeniem do nich innych odbiorników lub wykonane w specjalnym standardzie

§ 50

1. Dane osobowe przesyłane na nośnikach magnetycznych i optycznych oraz za pomocą systemów teleinformatycznych powinny być zabezpieczone w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.
2. Dane osobowe przesyłane po łączach telekomunikacyjnych na zewnątrz powinny być w miarę możliwości technicznych szyfrowane.

§ 51

Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych muszą być użytkowane z zachowaniem praw autorskich i posiadać licencje.

§ 52

Informatyk odpowiada za wyposażenie systemu informatycznego w mechanizmy uwierzytelniania użytkownika oraz za sprawowanie kontroli dostępu do danych osobowych jedynie osób upoważnionych.

§ 53

1. Ekrany monitorów powinny być w miarę możliwości wyposażone w wygaszacze zabezpieczone hasłem, które aktywują się automatycznie po upływie określonego czasu od ostatniego użycia komputera.

2. Ekrany monitorów powinny być ustawione w taki sposób, żeby w miarę możliwości uniemożliwić osobom nieupoważnionym odczyt wyświetlanych informacji.

3. Za spełnienie obowiązku określonego w ustępie 2 odpowiadają użytkownicy.

§ 54

1. Informatyk jest odpowiedzialny za to, aby dla każdej osoby, której dane osobowe są przetwarzane, system informatyczny zapewniał odnotowanie:

1) daty pierwszego wprowadzenia danych do systemu;
2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;
3) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
4) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
5) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

2. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

5. Do czasu spełnienia przez system informatyczny wszystkich wyżej wymienionych wymogów, system informatyczny powinien zapewnić odnotowanie :
1) daty pierwszego wprowadzenia danych ,
2) identyfikatora użytkownika wprowadzającego dane, chyba że dostęp do systemu informatycznego i przetwarzanych w nich danych posiada wyłącznie jedna osoba.

6. Do chwili spełnienia przez system informatyczny wszystkich wymogów określonych w niniejszym paragrafie, odnotowanie informacji określonych w ust. 1 pkt 3, 4 i 5 należy prowadzić w formie papierowej lub komputerowo poza systemem.

PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI

§ 55

1. Bieżących oraz okresowych przeglądów, napraw i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych, niewymagających angażowania zewnętrznych firm serwisowych, dokonuje Informatyk.

2. Przeglądów i konserwacji zbiorów danych osobowych dokonują użytkownicy, zgodnie
3. z indywidualnymi zakresami upoważnień i odpowiedzialności.

4. Informatyk w uzasadnionych przypadkach może opracować dla poszczególnych zasobów informatycznych szczegółowe procedury techniczno-eksploatacyjne, które stanowią podstawę do eksploatacji danego zbioru informatycznego w sposób odmienny
od określonego w niniejszej Instrukcji.

5. Procedury określone w ust. 3 nie dotyczą użytkowników, dotyczą wyłącznie Informatyka i upoważnionych pracowników służby informatycznej oraz osób upoważnionych przez Administratora Danych, które realizują prace techniczne

i administratorskie w stosunku do poszczególnych zasobów informatycznych.

§ 56

Prace dotyczące przeglądów, konserwacji i napraw, wymagające zaangażowania firm zewnętrznych są wykonywane za wiedzą Administratora Bezpieczeństwa Informacji przez

uprawnionych przedstawicieli tych firm pod nadzorem Informatyka lub upoważnionego użytkownika i w miarę możliwości bez dostępu do rzeczywistych danych osobowych.

§ 57

1. W przypadku, gdy zaistnieje potrzeba naprawy lub wymiany sprzętu komputerowego służącego do przetwarzania lub przechowywania danych osobowych należy usunąć dane w sposób uniemożliwiający ich odzyskanie.

2. Jeżeli nie ma możliwości usunięcia danych należy urządzenie uszkodzić w sposób uniemożliwiający ich odczytanie.

§ 58

Nadzór nad instalowaniem, sprawnym funkcjonowaniem i wymianą uszkodzonych urządzeń oraz ich likwidacją sprawuje Informatyk lub osoba wyznaczona przez Administratora Bezpieczeństwa Informacji.

POSTANOWIENIA KOŃCOWE

§ 59

Instrukcja jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym w żadnej formie.

§ 60

1. Użytkownicy są zobowiązani do zapoznania się z treścią Instrukcji.

2. Użytkownik zobowiązany jest złożyć oświadczenie, o tym, iż został zaznajomiony

z przepisami ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych oraz dokumentacją obowiązującą u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania.

3. Wzór oświadczenia, o którym mowa w ust. 2, stanowi załącznik nr 6 do Polityki bezpieczeństwa danych osobowych.

4. Oświadczenia przechowywane są w aktach osobowych.

§ 61

1. W sprawach nieuregulowanych w niniejszej instrukcji maja zastosowanie przepisy ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych.

2. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Instrukcji.

Załącznik Nr 1 do Instrukcji
Zarządzania Systemem Informatycznym

…….. ……..
(nazwa jednostki) (miejscowość, data,)

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 ze zm.)
upoważniam Panią/Pana* ……..*
do przetwarzania danych osobowych na wyznaczonym stanowisku pracy, zgodnie z powierzonymi obowiązkami oraz poleceniami Administratora danych.

Upoważnienie obejmuje prawo do ……

*(*Określić uprawnienia wg kryteriów: wglądu, wprowadzania, modyfikowania, udostępniania, usuwania danych osobowych*.)*

Zobowiązuje Panią/Pana* do przestrzegania przepisów dotyczących ochrony danych osobowych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych Polityki bezpieczeństwa danych osobowych oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Zobowiązuje również do zachowania poufności wszelkich informacji i danych uzyskanych w trakcie realizowania obowiązków pracowniczych. Obowiązek ten rozciąga się także na okres po ustaniu zatrudnienia.*

……. ……..…….
(podpis osoby upoważnionej) (podpis Administratora Danych)

* - niepotrzebne skreślić

Załącznik Nr 2 do Instrukcji
Zarządzania Systemem Informatycznym

TRYB PRZECHOWYWANIA I UDOSTĘPNIANIA HASEŁ INFORMATYKA

Ustala się następujący tryb postępowania z hasłami Informatyka:

1. Hasła Informatyka przechowywane są w formie pisemnej w zapieczętowanej kopercie.
2. Koperta jest złożona w specjalnej szafie, do której dostęp posiada wyłącznie Administrator Danych i osoby przez niego upoważnione.
3. Hasła, o których mowa w pkt 1 dają najwyższe uprawnienia administratorskie do korzystania i obsługi systemu informatycznego.
4. Nowe, aktualne hasło zabezpiecza się według procedur opisanych w pkt 1 i 2.
5. Koperta wraz z hasłem, które straciło ważność podlega zniszczeniu przy użyciu niszczarki dokumentów

6. Niszczenia, o którym mowa w pkt 5 dokonuje Informatyk w obecności Administratora Danych lub osoby przez niego upoważnionej.
7. W sytuacjach awaryjnych zaistniałych pod nieobecność Informatyka lub w razie jego niedyspozycji Administrator Danych udostępnia hasło osobie przez siebie wyznaczonej.

Załącznik Nr 3 do Instrukcji
Zarządzania Systemem Informatycznym

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Zakres upoważnienia: **O** - odczyt/wgląd, **W** - wprowadzanie, **M** - modyfikowanie, **K** - kopiowanie/powielanie, **U** - usuwanie/niszczenie, **P** – przekazywanie (udostępnianie/powierzanie do przetwarzania)

L.p.	Imię i nazwisko	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia	Login/ identyfikator	Uwagi
1.						
2.						
3.						
…						

Z A T W I E R D Z A M

……

Załącznik Nr 3 do Zarządzenia Nr 16/2013
Dyrektora Miejskiego Oświatowego Zespołu Ekonomicznego
w Tarnobrzegu z dnia 22.11.2013

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

1. Obszar, w którym przetwarzane są dane osobowe

Budynki, pomieszczenia lub części pomieszczeń

BUDYNEK

1) Tarnobrzeg ul. T.Kościuszki 30
2) pomieszczenia, w których przetwarzane są dane osobowe
   a) Miejski Oświatowy Zespół Ekonomiczny w Tarnobrzegu
   b) I piętro
   c) nr pomieszczeń :

102, 103, 104, 105, 106, 107, 108, 109, 110, 113, 114, 115 i 116

2. Wykaz zbiorów danych osobowych

L.p.	Nazwa zbioru	Nazwa programu
1.	Obsługa Finansowo-Księgowa Placówek Oświatowych	Vulcan ;- finanse - płace - kadry Pakiet Office
2.	Archiwum	
3.	Doskonalenie zawodowe	
4.	Komisja socjalna	
5.	Zamówienia publiczne	

3. Opis struktury zbioru danych osobowych

L.p.	Nazwa zbioru	Pola informacyjne		
		Nazwa pola	Zwartość	Powiązania z innymi polami
1.	Kadry	- Kwestionariusz osobowy	-nazwiska i imiona -imiona rodziców -data urodzenia -miejsce urodzenia -adres zamieszkania -nr ewidencji PESEL -nr NIP -zawód -wykształcenie	ze zbiorem płacowym

		-Umowa o pracę	-seria i nr dowodu osobistego -nr telefonu - warunki pracy -wartość wynagrodzenia	
------	----------	----------	----------	
2.	Płace	-lista płac	- wartość wynagrodzenia i potrąceń	
-----	----------	----------	----------	
3.	Księgowy	-Faktury	-nazwa -nr konta bankowego -adres -nr NIP	
		- Wyciągi bankowe	-nazwa -nr konta -wartość transakcji	

4. Sposób przepływu danych między poszczególnymi systemami (zbiorami)

Dane zgromadzone na serwerze i udostępniane za pośrednictwem sieci.

5. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych

Pomieszczenia usytułowane w budynku II piętrowym na I piętrze, na wspólnym korytarzu, do którego są drzwi zamykane na klucz. Każdy pokój zamykany na klucz. W pokojach z danymi kadrowo-płacowymi jak i na korytarzu głównym dodatkowo zainstalowano alarm ruchowy.
W pokojach umieszczone są komputery, z których każdy zabezpieczony jest hasłem, a dostęp do nich mają tylko osoby uprawnione. Dane w komputerach są udostępniane przez Administratora, każdy użytkownik ma dostęp tylko do tych danych, do których ma uprawnienia nadane przez Dyrektora jednostki.