POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

ROZDZIAŁ I
Postanowienia ogólne

§ 1

1. Polityka bezpieczeństwa zwana dalej „Polityką", określa środki techniczne i organizacyjne zastosowane przez Administratora Danych dla zapewnienia ochrony danych osobowych oraz tryb postępowania w przypadku stwierdzenia naruszenia zabezpieczenia danych osobowych w systemie informatycznym lub kartotekach, albo w sytuacji powzięcia podejrzenia o takim naruszeniu.
2. Polityka została opracowana zgodnie z wymogami określonymi w § 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

§ 2

1. Ilekroć w Polityce jest mowa o:

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

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

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 Starostwo Powiatowe w Wąbrzeźnie reprezentowany przez Starostę,

6) Staroście - rozumie się przez to Starostę Wąbrzeskiego,

7) Administratorze Bezpieczeństwa Informacji - rozumie się przez to osobę nadzorującą przestrzeganie zasad ochrony. przetwarzanych danych osobowych. Nadzoruje on stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, a także przeprowadza kontrole w zakresie określonym regulacjami wewnętrznymi Administratora Danych,

8) osobie odpowiedzialnej za prawidłowe funkcjonowanie sprzętu, oprogramowania i jego konserwację - rozumie się przez to informatyka odpowiedzialnego za powyższe zadania wyznaczonego przez Starostę, zwanego dalej „Administratorem Systemu Informatycznego",

9) komórce organizacyjnej - rozumie się przez to każdą wydzieloną organizacyjnie i funkcjonalnie komórkę wewnętrzną, zgodnie z regulaminem organizacyjnym,

10) użytkowniku - rozumie się przez to osobę wyznaczoną przez Starostę lub osobę przez niego upoważnioną do przetwarzania danych osobowych w systemie informatycznym oraz kartotekach,

10) pracowniku ochrony - rozumie się przez to osobę wykonującą zadania z zakresu ochrony osób i mienia na rzecz Administratora Danych,

11) 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 oraz gromadzone w kartotekach.

§ 3

1. 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.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu poniższych celów i zapewnić:

1) poufność danych - rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,

2) integralność danych - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

3) rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,

integralność systemu - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

3. Za przestrzeganie zasad ochrony i bezpieczeństwa danych w komórkach organizacyjnych odpowiedzialni są kierownicy tych komórek oraz osoby na stanowiskach samodzielnych.

§ 4

Realizację zamierzeń określonych w § 3 powinny zagwarantować następujące założenia:

1) wdrożenie procedur określających postępowanie osób upoważnionych 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 zabezpieczania systemów informatycznych i - w miarę możliwości organizacyjnych i techniczno-finansowych - wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemem informatycznym, które będą służyły wzmocnieniu bezpieczeństwa danych osobowych.

§ 5

Za naruszenie ochrony danych osobowych uważa się w szczególności:

1) nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują,

2) naruszenie lub próby naruszenia integralności danych rozumiane jako wszelkie modyfikacje, zniszczenia lub próby ich dokonania przez osoby nieuprawnione lub uprawnione działające w złej wierze lub jako błąd w działaniu osoby uprawnionej (np. zmianę zawartości danych, utratę całości lub części danych),

3) naruszenie lub próby naruszenia integralności systemu,

4) zmianę lub utratę danych zapisanych na kopiach zapasowych,

5) naruszenie lub próby naruszenia poufności danych lub ich części,

6) nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu),

7) udostępnienie osobom nieupoważnionym danych osobowych lub ich części,

8) zniszczenie, uszkodzenie lub wszelkie próby ingerencji nieuprawnionej w system informatyczny zmierzające do zakłócenia jego działania bądź pozyskania w sposób niedozwolony (lub w celach niezgodnych z przeznaczeniem) danych zawartych w systemie informatycznym lub kartotekach,

9) inny stan systemu informatycznego lub pomieszczeń, niż pozostawiony przez użytkownika po zakończeniu pracy,

Za naruszenie ochrony danych osobowych uważa się również włamanie do budynku lub pomieszczeń, w których przetwarzane są dane osobowe lub próby takich działań.

ROZDZIAŁ II

Przedsięwzięcia zabezpieczające przed naruszeniem ochrony danych osobowych

§ 6

1. Każdy użytkownik - przed dopuszczeniem do przetwarzania danych osobowych -podlega przeszkoleniu w zakresie przepisów o ochronie danych osobowych oraz wynikających z nich zadań oraz obowiązków.
2. Wszyscy użytkownicy podlegają okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (wymiana sprzętu na sprzęt nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji.

§ 7

1. Za organizację szkoleń, odpowiedzialny jest Administrator Bezpieczeństwa Informacji.
2. Szkolenia odbywają się na wniosek kierowników komórek organizacyjnych.

§ 8

1. Użytkownicy powinni mieć świadomość możliwości zaistnienia sytuacji naruszenia ochrony danych osobowych.
2. W tym celu należy:

    1) zwracać szczególną uwagę przy wchodzeniu i wychodzeniu z obiektu na podejrzane osoby lub samochody parkujące w pobliżu,

przestrzegać procedur związanych z otwieraniem i zamykaniem pomieszczeń, a także z wejściem do obszarów przetwarzania danych osobowych osób nieupoważnionych,

2) informować Administratora Bezpieczeństwa Informacji lub pracowników ochrony o podejrzanych osobach, tj.:

a) osobach zachowujących się nienormalnie np. nieodpowiednio ubranych do pory roku, dnia i pogody;

b) osobach przebywających w obiekcie bez wyraźnego celu;

c) osobach posiadających przy sobie podejrzane bagaże, w których mogą być ukryte niebezpieczne przedmioty;

d) przestrzegać zasad i procedur ochrony danych osobowych, w czasie pracy, a także po jej zakończeniu.

3. Kierownicy komórek organizacyjnych, a także osoby na stanowiskach samodzielnych oraz użytkownicy zobowiązani są, na podstawie dokonanej identyfikacj i ewentualnych zagrożeń, przedkładać Administratorowi Bezpieczeństwa Informacji projekty i propozycje stosownych rozwiązań, których celem jest zabezpieczenie przed naruszeniem ochrony danych osobowych.

§ 9

Do podstawowych zabezpieczeń przed naruszeniem ochrony danych osobowych należą:

1) ochrona obiektu przez wszystkie dni w roku,

2) wydzielenie pomieszczeń,

3) wyposażenie pomieszczeń w odpowiednie szafy,

4) zabezpieczenie wejść do pomieszczeń odpowiednimi zamkami,

5) zainstalowanie odpowiednich do zagrożeń systemów: alarmowych, monitoringu, telewizji przemysłowej, przeciwpożarowych itp.

§ 10

1. Stały dostęp do pomieszczeń, w których przetwarzane są dane osobowe, mają tylko użytkownicy.
2. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe, osób innych, niż wymienione w ust. 1, jest możliwy wyłącznie w obecności, co najmniej jednego użytkownika lub za zgodą Administratora Danych.
3. Zakaz wyrażony w ust. 2 dotyczy innych, niż określeni w ust. 1, pracowników Administratora Danych oraz pracowników służb technicznych, porządkowych, itp.

§ 11

1. Klucze do pomieszczeń przechowywane są w wyznaczonym pomieszczeniu.

2. Klucze wydawane są wyłącznie osobom do tego uprawnionym.
3. Klucze zapasowe do pomieszczeń, przechowywane są w specjalnej szafie i mogą być wydawane w sytuacjach awaryjnych.
4. Każdorazowe pobranie kluczy zapasowych podlega wpisowi do rejestru, w rejestrze odnotowuje się datę, godzinę i nazwisko osoby zdającej lub pobierającej klucze oraz jej podpis.
5. W przypadku podejrzenia zagrożenia pracownik ochrony może posłużyć się kluczami, o których mowa w ust. 1, w celu usunięcia zagrożenia; przed opuszczeniem Starostwa zobowiązany jest złożyć Administratorowi Bezpieczeństwa Informacji lub upoważnionej przez niego osobie pisemny raport na okoliczność użycia kluczy.

§12

1. Kartoteki należy przechowywać w przeznaczonych do tego szafach, do których dostęp mają wyłącznie użytkownicy.
2. Użytkownicy, o których mowa w ust. 1, odpowiedzialni są za rzetelne prowadzenie kartotek, ich kompletność oraz ochronę.

ROZDZIAŁ III
Przetwarzanie danych osobowych

§13

1. Przetwarzanie danych osobowych z użyciem stacjonarnego sprzętu komputerowego i kartotek odbywa się wyłącznie w obszarze przetwarzania danych, w pomieszczeniach Administratora Danych.
2. Przetwarzanie danych osobowych w urządzeniach przenośnych może odbywać się poza obszarem przetwarzania danych wyłącznie za zgodą Administratora Danych.
3. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe lub w którym przetwarzanie danych osobowych jest zabronione, stanowi załącznik nr 1 do Polityki.
4. Przetwarzanie, w tym udostępnianie danych osobowych jest prawnie dopuszczalne, jeżeli jest niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.
5. Podmiot występujący o udostępnienie danych osobowych 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 danych osobowych.

6. Przetwarzanie, w tym udostępnianie danych osobowych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą, oraz następuje w celach badań naukowych, dydaktycznych, historycznych lub statystycznych, z zachowaniem przepisów art. 23 i 25 ustawy o ochronie danych osobowych.
7. Udostępnienie danych osobowych może nastąpić jedynie za zgodą Administratora Danych lub osoby przez niego upoważnionej.

§14

W celu ograniczenia dostępu osób postronnych do pomieszczeń, w których zlokalizowano przetwarzanie danych osobowych, należy zapewnić, aby:

1) drzwi wejściowe były zabezpieczone tak, aby otwarcie z zewnątrz mogło nastąpić wyłącznie przez uprawnione osoby,

2) wydawanie kluczy pozwalających na wejście do Starostwa podlegało rejestracji, z jednoczesnym poświadczeniem przez osobę odbierającą, faktu otrzymania kluczy,

3) budynek był chroniony i monitorowany w systemie 24 godzinnym przez wszystkie dni w roku. Monitorowaniu powinny podlegać wyznaczone pomieszczenia w stopniu adekwatnym do ich przeznaczenia,

4) pomieszczenia, w których znajdują się serwery były wyposażone w miarę możliwości w sprawne systemy klimatyzacji, ochrony przeciwpożarowej i przeciwwłamaniowej,

5) pracownicy Administratora Danych oraz pracownicy ochrony są zobowiązani do przestrzegania zasad określających dopuszczalne sposoby przemieszczania się osób trzecich w obrębie pomieszczeń, w których przetwarzane są dane osobowe,

6) przebywanie osób trzecich w pomieszczeniach tworzących obszar przetwarzania danych może odbywać się wyłącznie w obecności użytkowników lub za zgodą Administratora Danych.

§15

Przebywanie użytkownika po godzinach pracy w pomieszczeniach, w których przetwarzane są dane osobowe jest dopuszczalne jedynie za zgodą Administratora Danych lub upoważnionej przez niego osoby.

§16

W trakcie prac technicznych wykonywanych przez osoby trzecie w pomieszczeniach, przetwarzanie danych osobowych jest zabronione.

§17

1. Administrator Bezpieczeństwa Informacji nadzoruje przestrzeganie zasad ochrony przetwarzanych danych osobowych.
2. W celu sprawnego wykonywania swoich zadań Administrator Bezpieczeństwa Informacji jest uprawniony do wnioskowania do Administratora Danych o wyznaczanie kierownikom komórek organizacyjnych oraz użytkownikom określonych zadań.
3. Kierownicy komórek organizacyjnych oraz pracownicy na stanowiskach samodzielnych zobowiązani są do przestrzegania przepisów o ochronie danych

osobowych na terenie podległych komórek organizacyjnych, a także do ścisłej współpracy z Administratorem Bezpieczeństwa Informacji. W tym celu zobowiązani są do:

1) pisemnego wnioskowania do Administratora Bezpieczeństwa Informacji o rejestracje nowych zbiorów danych osobowych,

2) pisemnego wnioskowania do Administratora Bezpieczeństwa Informacji o konieczności aktualizacji zbiorów danych osobowych.

3) okresowego składania pisemnej informacji z przebiegu bieżącej kontroli i oceny funkcjonowania mechanizmów zabezpieczeń i ochrony,

4) występowania z wnioskami w sprawie wprowadzenia niezbędnych zmian w zakresie ochrony danych osobowych.

§18

1. Szczegółowy wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania oraz stanowisk osób odpowiedzialnych za poszczególne zbiory zawiera załącznik nr 2 do Polityki.
2. Osoby odpowiedzialne za poszczególne zbiory zobowiązane są do pisemnego zgłaszania do Administratora Bezpieczeństwa Informacji konieczności aktualizacji zarejestrowanych zbiorów danych osobowych oraz opracowywania stosownych zgłoszeń zmian w zbiorach określonych w załączniku nr 2 do Polityki.
3. Administrator Systemu Informatycznego odpowiedzialny jest za pisemne zgłaszanie do Administratora Bezpieczeństwa Informacji nazw programów wykorzystywanych do przetwarzania danych osobowych określonych w załączniku nr 2 do Polityki.

§19

Opis struktury zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami zawiera załącznik nr 3 do Polityki.

ROZDZIAŁ IV

Kontrola przestrzegania zasad zabezpieczenia danych osobowych

§20

1. Administrator Bezpieczeństwa Informacji sprawuje nadzór nad przestrzeganiem zasad ochrony przetwarzanych danych osobowych.
2. W przypadku nieobecności Administratora Bezpieczeństwa Informacji, osobę zastępującą wyznacza Administrator Danych.
3. Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona dokonuje okresowych kontroli i oceny funkcjonowania mechanizmów zabezpieczeń oraz przestrzegania zasad postępowania w przypadku naruszenia ochrony danych osobowych.
4. Przedmiotem kontroli, o których mowa w ust. 3 powinno być w szczególności:

1) funkcjonowanie zabezpieczeń systemowych,

2) prawidłowość funkcjonowania mechanizmów kontroli dostępu do zbioru danych,

3) funkcjonowanie zastosowanych zabezpieczeń fizycznych,

4) zasady przechowywania kartotek,

5) zasady i sposoby likwidacji oraz archiwizowania zbiorów archiwalnych,

6) realizacja procedur wdrożonych przez Administratora Danych w zakresie ochrony danych osobowych.

5. Administrator Bezpieczeństwa Informacji prowadzi rejestr dokonywanych kontroli oraz ustaleń, wniosków i zaleceń z nich wynikających, a także nadzoruje ich wykonywanie.

6. Z kontroli, o których mowa w ust. 3 należy sporządzać protokoły, które przechowuje Administrator Bezpieczeństwa Informacji.

ROZDZIAŁ V

Postępowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych

§21

1. Przed przystąpieniem do pracy użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia ochrony danych osobowych.

2. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie Administratora Bezpieczeństwa Informacji lub upoważnionej przez niego osoby.

3. Obowiązek określony w ust. 2 ciąży również na pozostałych pracownikach Administratora Danych.

4. Postanowienia ust. 2 i 3 mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych gromadzonych w systemie informatycznym, jak i w kartotekach.

§22

1. Do czasu przybycia Administratora Bezpieczeństwa Informacji lub upoważnionej przez niego osoby, zgłaszający:

   1) powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów,

   2) zabezpiecza elementy systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osobom nieupoważnionym,

   3) podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

2. Postanowienia ust. 1 mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych.

§23

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona, po przybyciu na miejsce:

1) ocenia zastałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane osobowe oraz stan urządzeń, a także identyfikuje wielkość negatywnych następstw incydentu,

2) wysłuchuje relacji osoby, która dokonała powiadomienia,

2) podejmuje decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych. W uzasadnionych przypadkach niezwłocznie powiadamia Administratora Danych.

§24

1. Administrator Bezpieczeństwa Informacji lub upoważniona przez niego osoba sporządza z przebiegu zdarzenia raport, w którym powinny się znaleźć w szczególności informacje o:

1) dacie i godzinie powiadomienia,

2) godzinie pojawienia się w pomieszczeniach, w których przetwarzane są dane,

3) sytuacji, jaką zastał,

4) podjętych działaniach i ich uzasadnieniu.

2. Kopia raportu przekazywana jest bezzwłocznie Administratorowi Danych, a w przypadku, gdy raport sporządzony został przez osobę upoważnioną przez Administratora Bezpieczeństwa Informacji, także Administratorowi Bezpieczeństwa Informacji.

§25

1. Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona podejmuje kroki zmierzające do likwidacji naruszeń zabezpieczeń danych osobowych i zapobieżenia wystąpieniu ich w przyszłości. W tym celu:

1) w miarę możliwości przywraca stan zgodny z zasadami zabezpieczenia systemu,

2) relacjonuje Administratorowi Danych przedsięwzięte czynności,

3) o ile taka potrzeba zachodzi, postuluje wprowadzenie nowych form zabezpieczenia, a w razie ich wprowadzenia nadzoruje zaznajamianie z nimi osób dopuszczonych do przetwarzania danych osobowych.

2. W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej u Administratora Danych dyscypliny pracy, Administrator Bezpieczeństwa Informacji lub upoważniona przez niego osoba wnioskuje do Administratora Danych o wyjaśnienie wszystkich okoliczności incydentu i o podjęcie stosownych działań wobec sprawcy/sprawców.

§26

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik może kontynuować pracę dopiero po otrzymaniu pozwolenia od Administratora Bezpieczeństwa Informacji lub osoby przez niego upoważnionej.

§27

1. W przypadku zaginięcia komputera lub nośników magnetycznych, na których były zgromadzone dane osobowe, użytkownik posługujący się komputerem niezwłocznie powiadamia Administratora Bezpieczeństwa Informacji lub upoważnioną przez niego osobę, a w przypadku kradzieży występuje o powiadomienie jednostki policji.
2. W sytuacji, o której mowa w ust. 1 Administrator Bezpieczeństwa Informacji lub upoważniona przez niego osoba podejmuje niezbędne kroki do wyjaśnienia okoliczności zdarzenia, sporządza protokół z zajścia, który powinna podpisać także osoba, której skradziono lub, której zaginął sprzęt oraz powiadamia Administratora Danych.

3. W przypadku kradzieży komputera razem z nośnikiem magnetycznym Administrator Bezpieczeństwa Informacji lub upoważniona przez niego osoba podejmuje działania zmierzające do odzyskania utraconych danych oraz nadzoruje proces przebiegu wyjaśnienia sprawy.

§28

Osoba dopuszczona do przetwarzania danych osobowych za naruszenie obowiązków wynikających z niniejszej Polityki ponosi odpowiedzialność przewidzianą w przepisach aktów wewnętrznych Administratora Danych oraz na podstawie innych, odrębnych przepisów prawa.

ROZDZIAŁ VI
Postępowanie w wypadku klęski żywiołowej lub sytuacji kryzysowej

§29

Klęską żywiołową jest katastrofa, spowodowana działaniem sił przyrody np. takich jak ogień, huragan, woda lub ich przejawami.

§30

W przypadku wystąpienia zagrożenia powodującego konieczność przeprowadzenia ewakuacji osób lub mienia z pomieszczeń, w których przetwarzane są dane osobowe, mają zastosowanie przepisy niniejszego rozdziału oraz innych przepisów szczególnych.

§31

1. O zagrożeniu, jego skali i podjętych krokach zaradczych pracownik ochrony lub osoba kierująca ewakuacją zobowiązani są niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji w każdy możliwy sposób. W razie niemożności skontaktowania się z nim pracownik ochrony zawiadamia, co najmniej jedną z niżej wymienionych osób:
   1) osobę wyznaczoną przez Administratora Danych,
   2) Administratora Danych.
2. Numery telefonów Administratora Bezpieczeństwa Informacji i osób, z którymi należy się kontaktować na wypadek klęski żywiołowej powinny być znane pracownikom.

§32

Osoby biorące udział w akcji ratunkowej, mają prawo wejść do pomieszczeń, w których przetwarzane są dane osobowe bez dopełniania obowiązku, o którym mowa w § 10 ust. 2 Polityki.

§33

W przypadku ogłoszenia alarmu ewakuacyjnego użytkownicy, przebywający w pomieszczeniach, w których przetwarzane są dane osobowe, obowiązani są do przerwania pracy - w miarę możliwości przed opuszczeniem tych pomieszczeń do:

1) zamknięcia systemu informatycznego,
2) zabezpieczenia danych osobowych gromadzonych w kartotekach.

§34

1. W czasie trwania akcji ratunkowej i po jej zakończeniu Administrator Bezpieczeństwa Informacji oraz obecni użytkownicy powinni, w miarę możliwości, zabezpieczać dane osobowe przed nieuprawnionym do nich dostępem.
2. Obowiązek ten ciąży w równym stopniu na innych pracownikach Administratora Danych, obecnych przy akcji ratunkowej.

ROZDZIAŁ VII

Postanowienia końcowe

§35

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

§36

1. Kierownicy komórek organizacyjnych są obowiązani zapoznać z treścią Polityki każdego użytkownika.
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 potwierdzającego zaznajomienie użytkownika 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, stanowi załącznik nr 5 do Instrukcji.
4. Oświadczenia przechowywane są w aktach osobowych.

§37

1. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych.
2. Użytkownicy zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych osobowych 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 danych osobowych.

(podpis Administratora Danych)

Starosta

Krzysztof Mackiewicz

Załącznik nr 1 do Polityki bezpieczeństwa danych osobowych

SZCZEGÓŁOWY WYKAZ POMIESZCZEŃ

1. Przetwarzanie danych osobowych z użyciem stacjonarnego sprzętu komputerowego i kartotek odbywa się wyłącznie w obszarze przetwarzania danych, w pomieszczeniach Administratora Danych.
2. Obszarem przetwarzania danych są budynki, pomieszczenia lub ich części, w których przetwarzane są dane osobowe, znajdujące się w siedzibie Starostwa, ul. Wolności 44, 87-200, gdzie zlokalizowane są komórki organizacyjne Starostwa, główne systemy informatyczne, archiwa, kartoteki, z wyłączeniem pomieszczeń socjalno i ogólnie dostępnych, tj. korytarzy, toalet, magazynków, pomieszczeń gospodarczych, itp.
3. W pomieszczeniach Administratora Danych przetwarzanie danych jest zabronione, jeśli nie są zapewnione warunki ochrony danych osobowych określone w niniejszej Polityce.

(podpis Administratora Danych)

Załącznik nr 2 do Polityki bezpieczeństwa danych osobowych

WYKAZ ZBIORÓW DANYCH OSOBOWYCH

L.p.	Nazwa zbioru	Nazwa programu	Stanowisko osoby odpowiedzialnej za zbiór
1	ewidencja gruntów i budynków	EWOPIS	Kierownik WGGGiK
2	ewidencja wieczystych użytkowników gruntów Skarbu Państwa i Powiatu	Pakiet biurowy Office	Kierownik WGGGiK
3	wykaz budynków mieszkalnych i niemieszkalnych oraz obiektów zbiorowego zakwaterowania przekazanych do użytku	Kartoteka - spis	Kierownik WABiA
4	ewidencja wydanych pozwoleń na budowę	Kartoteka - spis	Kierownik WABiA
5	rejestr zalesień	Kartoteka - spis	Kierownik WROŚiGW
6	księga wodna	Kartoteka - spis	Kierownik WROŚiGW
7	rejestr łodzi rybackich	Kartoteka - spis	Kierownik WROŚiGW
8	rejestr kart wędkarskich	Kartoteka - spis	Kierownik WROŚiGW
9	ewidencja opłat melioracyjnych	Kartoteka - spis	Kierownik WROŚiGW
10	rejestr o dopuszczalnej emisji	Kartoteka - spis	Kierownik WROŚiGW
11	ewidencja osób mających zobowiązania wobec Skarbu Państwa i Powiatu	RADIX	Skarbnik Powiatu
12	ewidencji pojazdów	CEPiK	Kierownik WK
13	Ewidencja kierowców	CEPiK	Kierownik WK
14	rejestr tablic rejestracyjnych	CEPiK	Kierownik WK
15	rejestr dowodów rejestracyjnych	CEPiK	Kierownik WK
16	rejestr wydanych międzynarodowych praw jazdy	CEPiK	Kierownik WK
17	rejestr osób które zmieniły imię lub nazwisko	Kartoteka - spis	Inspektor w Wydziale Organizacyjnym
18	listy poborowych	Kartoteka - spis	Inspektor w Wydziale Organizacyjnym
19	Rejestr podmiotów prowadzących bazy danych oświatowych	SIO System Informacji Oświatowej	Inspektor w Wydziale Oświaty

Załącznik nr 3 do Polityki bezpieczeństwa danych osobowych

STRUKTURA ZBIORÓW DANYCH OSOBOWYCH

I. Szczegółowy opis struktury zbiorów danych osobowych określonych w załączniku nr 2 wraz ze wskazaniem poszczególnych pól informacyjnych i powiązań między nimi znajduje się w dokumentacji technicznej będącej w posiadaniu Administratora Systemu Informatycznego i autorów oprogramowania.

II. Programem wykorzystywanym do przetwarzania danych osobowych u Administratora Danych jest między innymi pakiet biurowy Office.

III. Dane osobowe przetwarzane są w aplikacjach:

   a. Edytor tekstu,

   b. Arkusz kalkulacyjny,

IV. Aplikacje pakietu Office oferują szeroki zakres możliwości rejestrowania:

   a. daty wprowadzenia danych,

   b. identyfikatora użytkownika,

   c. źródła danych,

   uzależniony od konfiguracji, wersji, zainstalowanych składników, aktualizacji oraz poprawek.