Zarządzenie Nr 122 / 2013
Starosty Wałbrzyskiego
z dnia 28 listopada 2013 roku

w sprawie: wprowadzenia do stosowania w Starostwie Powiatowym w Wałbrzychu polityki bezpieczeństwa przetwarzania danych osobowych

Na podstawie art. 34 ust.1 ustawy z dnia 05 czerwca 1998 roku o samorządzie powiatowym (tj. Dz.U. z 2013 r., poz.595 z późn. zm.), art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) i rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz.1024) zatwierdzam i wprowadzam do stosowania następujące dokumenty:

§ 1

„Politykę bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym w Starostwie Powiatowym w Wałbrzychu" stanowiącą załącznik Nr 1 do niniejszego Zarządzenia.

§ 2

1. „Instrukcję zarządzania systemem informatycznym w Starostwie Powiatowym w Wałbrzychu" stanowiącą załącznik Nr 2 do niniejszego Zarządzenia.
2. „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych Pojazd i Kierowca w Starostwie Powiatowym w Wałbrzychu" stanowiącą załącznik Nr 3 do niniejszego Zarządzenia.

§ 3

Wykonanie i nadzór nad niniejszym zarządzeniem powierzam Administratorowi Bezpieczeństwa Informacji.

§ 4

Traci moc Zarządzenie Nr 18/2011 Starosty Wałbrzyskiego z dnia 09 lutego 2011 roku w sprawie wprowadzenia do stosowania w Starostwie Powiatowym w Wałbrzychu „Polityki bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym i tradycyjnym w Starostwie Powiatowym w Wałbrzychu" i „Instrukcje zarządzania systemem informatycznym w Starostwie Powiatowym.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA
Józef Pilsa

Sprawdzono pod względem formalno-prawnym

RADCA PRAWNY
Monika Sąsiada
nr OP-1055

Załącznik Nr 2
do Zarządzenia Nr 122 /2013
Starosty Wałbrzyskiego
z dnia 28 listopada 2013 roku

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM W STAROSTWIE POWIATOWYM W WAŁBRZYCHU

Wałbrzych, listopad 2013 roku

Spis treści

I. PODSTAWA PRAWNA

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024). Art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).

II. WSTĘP

Instrukcja określa sposób zarządzania systemem informatycznym wykorzystywanym do przetwarzania danych osobowych przez administratora danych w celu zabezpieczenia danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnianiem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem, opisuje nadawanie uprawnień użytkownikom, określa sposoby pracy w systemie informatycznym oraz czynności mające wpływ na zapewnienie bezpieczeństwa systemu informatycznego Starostwa Powiatowego w Wałbrzychu.

III. PODSTAWOWE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. Przetwarzanie danych osobowych odbywa się zgodnie z obowiązującą ustawą o ochronie danych osobowych oraz wykonawczymi dokumentami normatywnymi.
2. Osobą odpowiedzialną za bezpieczeństwo danych w systemach informatycznych przetwarzających dane osobowe jest administrator bezpieczeństwa informacji.
3. Naczelnik Wydziału odpowiada za egzekwowanie i przestrzeganie zapisów ustawy o ochronie danych osobowych w pracy przez pracowników związanych z przetwarzaniem danych osobowych i ich ochroną.
4. Przetwarzanie danych osobowych jest możliwe tylko przez uprawnione osoby w wyznaczonym przez administratora danych obszarze, podlegającym szczególnej ochronie i zabezpieczeniu.
5. Pracownicy przetwarzający dane osobowe zobowiązani są do zachowania ich w tajemnicy jak również sposobów ich zabezpieczenia.

IV. DEFINICJE

1. **Zbiór danych osobowych** - należy przez to rozumieć każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów.
2. **Dane osobowe** – są to wszystkie informacje odnoszące się do zidentyfikowania lub możliwej do zidentyfikowania osoby fizycznej.
3. **Przetwarzanie danych osobowych** - należy przez to rozumieć wszystkie operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie (nawet, jeśli faktycznie z nich się nie korzysta), opracowywanie, zmienianie, udostępnianie i usuwanie, które wykonuje się zwłaszcza w systemach informatycznych.

4. **Usuwanie danych osobowych** – należy przez to rozumieć wykonanie tej czynności w sposób niepozwalający na odtworzenie ich treści, czyli tak aby po dokonaniu usunięcia danych niemożliwe było zidentyfikowanie osób, których dotyczą.
5. **System informatyczny** - należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
6. **Zabezpieczenie systemu informatycznego** - należy przez to rozumieć zespół stosowanych środków technicznych i fizycznych w celu zabezpieczenia zasobów oraz ochrony danych przed ujawnieniem, zniszczeniem, utratą, a także nieuprawnionym dostępem i przetwarzaniem.
7. **Administrator danych osobowych** - należy przez to rozumieć osobę decydującą o celach i środkach przetwarzania danych - Starosta Wałbrzyski.
8. **Administrator bezpieczeństwa informacji** - należy przez to rozumieć osobę wyznaczoną przez administratora danych odpowiedzialną za bezpieczeństwo danych, w tym szczególnie za przeciwdziałanie dostępowi do systemu osób niepowołanych oraz za podejmowanie działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.
9. **Administrator systemu** - pracownik – informatyk odpowiedzialny za funkcjonowanie systemu informatycznego, systemu operacyjnego oraz generację haseł dostępu, ze szczególnym uwzględnieniem bezpieczeństwa i ochrony danych osobowych.
10. **Użytkownik systemu informatycznego** - należy przez to rozumieć wyznaczoną przez administratora bezpieczeństwa informacji osobę odpowiedzialną za organizację i ochronę danych i systemu na określonym stanowisku pracy.

V. POZIOM BEZPIECZEŃSTWA

Uwzględniając kategorie danych osobowych oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie informatycznym połączonym z siecią publiczną, wprowadza się ,,poziom wysoki" bezpieczeństwa w rozumieniu §6 rozporządzenia.

VI. PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM ORAZ OSOBY ODPOWIEDZIALNE ZA TE CZYNNOŚCI.

Podstawowe zasady nadawania uprawnień:

1. Upoważnienia do przetwarzania danych osobowych wydawane są na podstawie pisma naczelnika wydziału informującego o osobach wyznaczonych do przetwarzania danych osobowych w zbiorach i zakresie przetwarzania danych.

   Wniosek o wydanie upoważnienia powinien zawierać:

- nazwisko i imię, stanowisko służbowe osoby wyznaczonej do przetwarzania danych osobowych, (w przypadku osób z zewnątrz mających obsługiwać określone zbiory danych osobowych – wskazanie podstawy do wydania upoważnienia, np. umowa, porozumienie, itp.)
- nazwę zbioru danych osobowych,
- zakres upoważnienia,

- termin obowiązywania upoważnienia

2. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych zobowiązany jest:

- zapoznać się z Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity z 2002 r. Dz. U. Nr 101, poz. 926 z późn. zm.)
- podpisać oświadczenie o zapoznaniu się z postanowieniami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. z 2002 roku Dz. U. Nr 101 poz. 926, z późn. zm.) i jej przestrzegania w trakcie zatrudnienia jak również po jego ustaniu.
- być przeszkolonym w zakresie ochrony danych osobowych przez Administratora Bezpieczeństwa Informacji.
- zapoznać się z „Polityką bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym w Starostwie Powiatowym w Wałbrzychu".
- zapoznać się z niniejszym dokumentem.

3. Administrator Systemu Informatycznego przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego upoważnienia (wniosku) określającego zakres uprawnień pracownika, którego wzór stanowi **załącznik nr 1**, z wyłączeniem osób kierujących Starostwem.
4. Administrator Systemu jest zobowiązany upoważnić co najmniej jednego pracownika - do rejestracji użytkowników w systemie informatycznym w czasie swojej nieobecności dłuższej niż 21 dni.
5. Rejestracja użytkownika, polega na nadaniu unikalnego identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.
6. Wyrejestrowanie użytkownika z systemu informatycznego dokonuje administrator systemu na wniosek przełożonego **załącznik nr 1**, któremu pracownik podlega z podaniem daty oraz przyczyny odebrania uprawnień, zatwierdzonego przez Administratora Bezpieczeństwa Informacji.
7. Wyrejestrowanie, o którym mowa w ust. 6, może mieć charakter czasowy lub trwały.
8. Wyrejestrowanie następuje przez:

1) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe)
2) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

9. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego może być:

1) wypowiedzenie umowy o pracę;
2) wszczęcie postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych osobowych.
3) zawieszenie w pełnieniu obowiązków służbowych

10. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.

11. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jej hasło.
12. Administrator Systemu Informatycznego zobowiązany jest do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym, rejestr stanowi **załącznik nr 2**.

VII. STOSOWANE METODY I ŚRODKI UWIERZYTELNIANIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM.

1. Identyfikator składa się z co najmniej sześciu znaków i budowany jest zgodnie z zasadą ustaloną przez administratora sytemu, która to znana jest także administratorowi bezpieczeństwa informacji.
2. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika administrator systemu za zgodą administratora bezpieczeństwa informacji, nadaje inny identyfikator odstępując od zasady określonej w ust.1.
3. W systemie stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji.
4. Identyfikator użytkownika w aplikacji (o ile działanie aplikacji na to pozwala), powinien być tożsamy z tym, jaki jest mu przydzielany w sieci lokalnej.
5. Naczelnicy wydziałów zobowiązani są pisemnie informować Administratora Bezpieczeństwa Informacji o każdej zmianie dotyczącej podległych pracowników mających wpływ na zakres posiadanych uprawnień w systemie informatycznym.
6. Bezpośredni dostęp do systemu informatycznego może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
7. Hasło użytkownika powinno być zmieniane nie rzadziej niż co 30 dni.
8. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
9. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.
10. Hasło użytkownika utrzymuję się również w tajemnicy po upływie ich ważności.
11. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
12. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do powiadomienia Administratora Systemu w celu nadania nowego hasła.
13. Hasło powinno składać się z niepowtarzalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne o ile system informatyczny na to pozwala. Hasło nie może być identyczne z identyfikatorem użytkownika w jakiejkolwiek formie(pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę itp.), ani z jego imieniem lub nazwiskiem.
14. Zakazuję się stosować haseł, które użytkownik stosował uprzednio w okresie minionego roku, imion osób z najbliższej rodziny, ogólnie dostępnych informacji o użytkowniku takich jak numer

telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy na której mieszka lub pracuje, przewidywanych sekwencji z klawiatury (np.: „ASDFG" i „12345" itp.)

15. Zmiany hasła nie wolno zlecać innym osobom, oprócz Administratora Systemu.
16. Nie należy korzystać z opcji zapamiętywania hasła w systemie.
17. Hasło administratora systemu przechowywane jest w zamkniętej kopercie w szafie pancernej w zabezpieczonym pomieszczeniu, do którego mają dostęp wyłącznie Starosta, Administrator Systemu oraz Administrator Bezpieczeństwa Informacji.

VIII. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU.

1. Rozpoczęcie pracy na stacji roboczej następuje po włączeniu napięcia w listwie podtrzymującej napięcie (w przypadku posiadania listwy), włączeniu zasilacza awaryjnego (UPS) i komputera, a następnie wprowadzeniu identyfikatora indywidualnego oraz hasła identyfikatora znanego tylko użytkownikowi.
2. W pomieszczeniu, w którym przetwarzane są dane osobowe, mogą znajdować się osoby postronne tylko za zgodą i w towarzystwie użytkownika albo Administratora Bezpieczeństwa Informacji.
3. Przed osobami postronnymi należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwiać podgląd), wydruki leżące na biurkach oraz w otwartych szafach.
4. Monitory komputerów wyposażone są we włączające po 5 minutach od przerwania pracy wygaszacze ekranu. Wznowienie wyświetlenia następuje dopiero po wprowadzeniu odpowiedniego hasła.
5. W przypadku opuszczenia stanowiska pracy użytkownik obowiązany jest wylogować się z systemu aktywizować lub w inny sposób zablokować stację roboczą.
6. Obowiązuje zakaz robienia kopii całych zbiorów danych. Całe zbiory danych mogą być kopiowane tylko przez Administratora Systemu lub automatycznie przez system, z zachowaniem procedur ochrony danych osobowych.
7. Jednostkowe dane mogą być przekazywane pocztą elektroniczną między komputerami Administratora Danych, a komputerami przenośnymi użytkowników tylko po ich zabezpieczeniu hasłem.
8. Wypisy ze zbiorów danych udostępniane na podstawie art. 29 ustawy podmiotom nie będącym odbiorcami danych można przesyłać poczta elektroniczną tylko w postaci zaszyfrowanej.
9. Obowiązuje zakaz wynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz obszernych z nich wypisów, nawet w postaci zaszyfrowanej.
10. Przetwarzając dane osobowe, należy odpowiednio często robić kopie robocze danych, na których się właśnie pracuje, tak aby zapobiegać ich utracie.
11. Zakończenie pracy na stacji roboczej następuje po wprowadzeniu danych programów, a następnie prawidłowym zamknięciu aplikacji uruchomionych oraz wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w zasilaczu awaryjnym (UPS) i listwie (jeżeli jest podłączona).

12. Przed opuszczeniem pokoju należy:

a) zniszczyć w niszczarce lub schować do zamykanych na klucz szaf wszelkie wykonane wydruki zawierające dane osobowe,

b) schować do zamykanych na klucz szaf akta zawierające dane osobowe,

c) umieścić klucze do szaf w ustalonym, przeznaczonym do tego miejscu,

d) zamknąć okna.

13. Opuszczając pokój, należy zamknąć za sobą drzwi na klucz. Jeśli niemożliwe jest umieszczenie wszystkich zawierających dane osobowe dokumentów w zamykanych szafach, to należy powiadomić o tym Sekretarza Powiatu lub Naczelnika Wydziału Organizacyjnego i Spraw Obywatelskich, który zgłasza osobom sprzątającym jednorazową rezygnację z wykonania usługi sprzątania.

14. Jeżeli jest to możliwe, to przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują procedury określone w niniejszej instrukcji dotyczące pracy na komputerach stacjonarnych.

15. Użytkownicy, którym zostały powierzone komputery przenośne powinny chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych; szczególną ostrożność należy zachować podczas ich transportu.

16. Obowiązuje zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone.

17. Praca na komputerze przenośnym możliwa jest po wprowadzeniu hasła i indywidualnego identyfikatora użytkownika.

18. Użytkownicy są zobowiązani zmieniać hasła w komputerach przenośnych nie rzadziej niż co 30 dni.

19. Obowiązuje zakaz przetwarzania na komputerach przenośnych całych zbiorów danych lub obszernych z nich wypisów, nawet w postaci zaszyfrowanej,

20. Obowiązuje zakaz samodzielnej modernizacji oprogramowania i sprzętu w powierzonych komputerach stacjonarnych oraz przenośnych. Wszelkie zmiany mogą być dokonywane tylko pod nadzorem Administratora Systemu, stosownie do wymagań niniejszej instrukcji. W razie wystąpienia usterek w pracy komputerów przenośnych lub w razie wystąpienia konieczności aktualizacji ich oprogramowania należy zgłosić to Administratorowi Systemu.

21. Komputery stacjonarne oraz przenośne wyposażone są w odpowiednie programy ochrony antywirusowej, których aktualizację pobierana jest automatyczne lub przez Administratora Systemu.

IX. PROCEDURA POSTĘPOWANIA W SYTUACJI NARUSZENIA BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO

1. Użytkownik zobowiązany jest zawiadomić Administratora Systemu lub Administratora Bezpieczeństwa Informacji o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu, a w szczególności o:

1) naruszeniu hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzania hasła),
2) częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień,
3) braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera,
4) wykryciu wirusa komputerowego,
5) zauważeniu elektronicznych śladów próby włamania do systemu informatycznego Administratora Danych,
6) znacznym spowolnieniu działu informatycznego,
7) podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe,
8) zmianie położenia sprzętu komputerowego,
9) zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf.

2. Do czasu przybycia na miejsce Administratora Bezpieczeństwa Informacji lub Administratora Systemu:

1) jeżeli istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego zdarzenia a następnie uwzględnić w działaniu również ustalenie jego przyczyny lub sprawców,
2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
3) zaniechać – jeżeli to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
4) zastosować się do instrukcji i regulaminów lub dokumentacji aplikacji, jeśli odnoszą się one do zaistniałego przypadku,
5) przygotować opis incydentu,
6) nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji lub Administratora Systemu.

3. Administrator Systemu przyjmujący zawiadomienie jest obowiązany niezwłocznie poinformować Administratora Bezpieczeństwa Informacji o naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu.

4. Administrator Bezpieczeństwa Informacji po otrzymaniu zawiadomienia, o którym mowa w ust.3, powinien niezwłocznie:

1) przeprowadzić postępowanie wyjaśniające, w celu ustalenia okoliczności naruszenia ochrony danych osobowych,
2) podjąć działania chroniące system przed ponownym naruszeniem,
3) w przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu sporządzić raport naruszenia bezpieczeństwa systemu informatycznego Administratora Danych, a następnie niezwłocznie przekazać jego kopie Administratorowi Danych,

5. Administrator Bezpieczeństwa Informacji w uzgodnieniu z Administratorem Systemu może zarządzić, w razie potrzeby, odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części.
6. W razie odtwarzania danych z kopii zapasowych Administrator Systemu obowiązany jest upewnić się, że odtwarzane dane zapisane zostały przed wystąpieniem incydentu; dotyczy to zwłaszcza przypadków infekcji wirusowej.
7. Administrator danych po zapoznaniu się z raportem, o którym mowa w ust. 4 pkt 3, podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych, szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego Administratora Danych bądź zastosowaniu środków ochrony fizycznej.
8. Administrator Bezpieczeństwa Informacji i Administrator Systemu zobowiązani są do informowania Administratora Danych o awariach systemu informatycznego, zauważonych przypadkach naruszenia niniejszej instrukcji przez użytkowników, a zwłaszcza o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami, nieprzestrzegania zasad używania oprogramowania antywirusowego, niewłaściwego wykorzystania sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z procedurami ochrony danych osobowych.
9. Administrator Bezpieczeństwa Informacji składa raz w roku Administratorowi Danych kompleksową analizę zarządzania systemem informatycznym.

X. PROCEDURY TWORZENIA KOPII ZAPASOWYCH

Kopie zapasowe tworzy się:

1) codziennie – w przypadku programu EWID2007, INTRADOK
2) nie rzadziej niż raz na miesiąc – w wypadku zbioru programu Wydawanie licencji, zezwoleń, zaświadczeń na wykonywanie transportu drogowego, PEFS, Płace/Kadry Probit, Płatnik – ZUS, FK-2000.
3) raz w roku kalendarzowym robiona jest kopia na płytach DVD, jeżeli na to pozwala wielkość danych zgromadzonych w ciągu roku - System Informacji Oświatowej

2. Wybrane kopie wykonywane są po zakończeniu pracy wszystkich użytkowników w sieci komputerowej.
3. Kopia bezpieczeństwa wykonywana jest na płytach CD/DVD lub innym nośniku danych.
4. W przypadku wykonywania zabezpieczeń długoterminowych na taśmach magnetycznych lub płytach CD/DVD, nośniki te należy dwa razy w roku sprawdzać pod kątem ich dalszej przydatności.
5. Stwierdzenie utraty przez kopie awaryjne waloru przydatności do celu, o którym mowa w ust.4, upoważnia Administratora Systemu do ich zniszczenia.

XI. SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ICH KOPII ZAPASOWYCH

1. Elektroniczne nośniki informacji.

1) Dane osobowe w postaci elektronicznej – zapisywane na dyskietkach, dyskach magnetooptycznych czy dyskach twardych nie są wynoszone poza siedzibę Starostwa.

2) Wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych określonych w Polityce bezpieczeństwa systemów informatycznych do przetwarzania danych osobowych.
3) Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych.
4) Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe uszkadza się w sposób mechaniczny uniemożliwiając ich odczytanie.
5) Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych pozbawia się wcześniej zapisu tych danych.
6) Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.
7) Zakazuje się przetwarzania danych osobowych na zewnętrznych nośnikach magnetycznych, optycznych i innych oraz ich przesyłania pocztą, elektroniczną bez ich uprzedniego zaszyfrowania.
8) Na nośnikach, o których mowa w pkt. 7, dopuszczalne jest przetwarzanie jedynie jednostkowych danych osobowych.
9) W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym na swoim komputerze.
10) Nośniki magnetyczne z zaszyfrowanymi, jednostkowymi danymi osobowymi są – na czas ich użyteczności – przechowywane w zamkniętych na klucz szafach, a po ich wykorzystaniu dane na nich zawarte są trwale usuwane lub nośniki te są niszczone.
11) Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione do przetwarzania danych osobowych.
12) Kopie zapasowe programów, których przydatność nie nadaje się do dalszego wykorzystania są trwale niszczone mechanicznie w niszczarce.

2. Kopie zapasowe.

1) Kopie bezpieczeństwa są przechowywane w wyznaczonych pomieszczeniach wydziałów, które je wykonały.

3. Wydruki.

1) W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.
2) Pomieszczenia, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy.
3) Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

XII. SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO ORAZ WIRUSAMI KOMPUTEROWYMI

1. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe pracujące w trybie monitora (ciągła praca w tle).
2. Każdy e-mail oraz załączniki muszą być sprawdzone przez program antywirusowy pod kątem obecności wirusów.
3. Definicje wzorców wirusów aktualizowane są nie rzadziej niż raz w miesiącu.
4. Jeżeli oprogramowanie antywirusowe pozwala, to należy ustawić harmonogram zadań tak, aby raz w miesiącu lub więcej razy sprawdzał daną jednostkę komputerową pod kątem obecności wirusów.
5. Do obowiązków Administratora Systemu należy aktualizacja oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji wirusów dokonywanych przez to oprogramowanie.
6. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć.
7. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
8. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.
9. Administrator Systemu Informatycznego przeprowadza cyklicznie kontrole antywirusowe na wszystkich komputerach – minimum co trzy miesiące.
10. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku stwierdzenia nieprawidłowości zgłoszonych przez pracownika w funkcjonowaniu sprzętu komputerowego lub oprogramowania.
11. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe na którym wykryto wirusa oraz wszystkie posiadane przez użytkownika nośniki.
12. Użytkownik jest obowiązany zawiadomić administratora systemu o pojawiających komunikatach wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.
13. Użytkownicy mogą korzystać z zewnętrznych nośników danych tylko po uprzednim sprawdzeniu zawartości nośnika oprogramowaniem antywirusowym.

XIII. KONTROLA NAD WPROWADZANIEM, DALSZYM PRZETWARZANIEM I UDOSTĘPNIANIEM DANYCH OSOBOWYCH

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom uprawnionym.
2. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną.

3. Aplikacje danych osobowych do obsługi baz danych osobowych powinny zapewniać odnotowanie informacji o udzielonych odbiorcom danych. Zakres informacji powinien obejmować co najmniej dane odbiorcy, datę wydania, zakres udostępnionych danych.

XIV. PROCEDURA WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

1. Przeglądu i konserwacji systemu dokonuje administrator systemu doraźnie.
2. Przeglądu i konserwacji urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonych przez producenta sprzętu.
3. Nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny powinny być przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić Administratora Bezpieczeństwa Informacji.
4. Przeglądu pliku zawierającego raport dotyczący działalność aplikacji bądź systemów serwerowych (log systemowy) Administrator Systemu dokonuje nie rzadziej niż raz na miesiąc.
5. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy współudziale Administratora Systemu nie rzadziej niż raz na miesiąc.
6. W przypadku działań konserwacyjnych, awarii oraz napraw Administrator Bezpieczeństwa Informacji prowadzi „Dziennik systemu informatycznego Starostwa Powiatowego w Wałbrzychu" - **załącznik nr 3**
7. Wpisów do dziennika może dokonywać Administrator Danych, Administrator Bezpieczeństwa Informacji lub Administrator Systemu.

XV. NAPRAWA URZĄDZEŃ KOMPUTEROWYCH Z CHRONIONYMI DANYMI OSOBOWYMI

1. Wszelkie naprawy urządzeń komputerowych oraz zmiany w systemie informatycznym Administratora Danych przeprowadzane są – jeżeli jest to możliwe – przez Administratora Systemu.
2. Naprawy i zmiany w systemie informatycznym Administratora Danych przeprowadzane przez serwisanta prowadzone są pod nadzorem Administratora Systemu, jeżeli jest to możliwe – w siedzibie administratora danych lub poza siedzibą Administratora Danych, po uprzednim nieodwracalnym usunięciu danych w nich przetwarzanych, a jeśli wiązałoby się to z nadmiernymi utrudnieniami, to po podpisaniu umów powierzenia przetwarzania danych osobowych.
3. Jeśli nośnik danych (dysk, dyskietka, płyta lub inne) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, to należy go zniszczyć mechanicznie.

XVI. INNE ŚRODKI BEZPIECZEŃSTWA

1. Obszar przetwarzania danych osobowych w systemie informatycznym tworzą pomieszczenia biurowe Starostwa Powiatowego przy Alei Wyzwolenia 20, 22, 24.
2. W obszarze przetwarzania danych osobowych pokoje na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych są zamykane na klucz.

Pomieszczenia, w których jest zakaz przebywania osobom nieupoważnionym oznakowane są napisem „zakaz wstępu osobom nieupoważnionym".

3. Budynek Starostwa Powiatowego w Wałbrzychu przy Alei Wyzwolenia 20, 22, 22a, 24 podlega całodobowej ochronie, którą zapewnia Firma Ekotrade. Wszystkie drzwi wejściowe do budynku zamykane są na klucz po wyjściu pracowników Starostwa. Wstęp do budynku jest kontrolowany.
4. Sprzęt komputerowy, w którym przetwarzane są dane osobowe zabezpieczony jest przed dostępem do systemu informatycznego przez Firewall oraz zainstalowany na każdej stacji roboczej program antywirusowy oraz instalowanie tylko programów oryginalnych.
5. Przed utratą danych spowodowaną awarią zasilania zastosowano na wybranych stanowiskach urządzenia podtrzymujące zasilanie UPS.
6. Dane osobowe przetwarzane w systemie informatycznym przetwarzane są w specjalistycznych programach, które wymuszają procedury postępowania w wykonywaniu kopii i archiwizacji, a tym samym uniemożliwiają wykonanie kopii przez osoby nieupoważnione i na innym nośniku niż jest do tego przeznaczony.

XVII. POSTANOWIENIA KOŃCOWE

1. W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.
2. Naruszenie obowiązków wynikających z niniejszej instrukcji oraz przepisów o ochronie danych osobowych może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym, w szczególności wynikającym z art. 49-54 ustawy.

WNIOSEK
O NADANIE UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

☐ Nowy użytkownik	☐ Modyfikacja uprawnień	☐ Odebranie uprawnień w systemie informatycznym

Imię i nazwisko użytkownika:	**Wydział/biuro/samodzielne stanowisko**
Opis i zakres uprawnień użytkownika w systemie informatycznym	
Data wystawienia:	Podpis bezpośredniego przełożonego użytkownika systemu:
Podpis Administratora Systemu:	Akceptacja ABI

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRACY W SYSTEMIE INFORMATYCZNYM ORAZ UPOWAŻNINYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Nazwisko, Imię	System/aplikacja	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania uprawnień	Data ustania uprawnień	Identyfikator użytkownika

Dziennik zawiera opisy wszelkich zdarzeń istotnych dla działania systemu informatycznego w szczególności:

- w przypadku awarii – opis awarii, przyczyna awarii, szkody wynikłe na skutek awarii, sposób usunięcia awarii, opis systemu po awarii, wnioski,
- w przypadku konserwacji systemu – opis podjętych działań, wnioski.

DZIENNIK SYSTEMU INFORMATYCZNEGO STAROSTWA POWIATOWEGO W WAŁBRZYCHU

L.p.	Data i godzina zdarzenia	Opis zdarzenia	Podjęte działania/wnioski	Podpis

Zakończenie

Dokument pn. „Instrukcja zarządzania systemem informatycznym w Starostwie Powiatowym w Wałbrzychu" została opracowane i przekazana do stosowania osobom upoważnionym do przetwarzania zbiorów danych osobowych w systemie informatycznym. Naczelnicy Wydziałów w których użytkowane są zbiory danych osobowych odpowiadają za zakomunikowanie „Instrukcji" pracownikom i egzekwowanie przestrzegania jej zapisów w pracy przez pracowników związanych z przetwarzaniem danych osobowych i ich ochroną.

STAROSTA
Józef Pilsa

Załącznik Nr 1
do Zarządzenia Nr 122 /2013
Starosty Wałbrzyskiego
z dnia 28 listopada 2013 roku

POLITYKA
BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH
W SYSTEMIE INFORMATYCZNYM
W STAROSTWIE POWIATOWYM W WAŁBRZYCHU

Wałbrzych, listopad 2013

SPIS TREŚCI

PODSTAWA PRAWNA:

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity z 2002 r. Dz. U. Nr 101 poz. 926 z późn. zm.)

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (Dz. U. Nr 100 poz. 1024) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

I. WSTĘP

Zgodnie z art. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity z 2002 r. Dz. U. Nr 101 poz. 926 z późn. zm.) oraz § 3 i § 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) Starosta Wałbrzyski będący administratorem danych, został zobowiązany do opracowania i wdrożenia „Polityki bezpieczeństwa przetwarzania danych osobowych" zwanej dalej „Polityką bezpieczeństwa". Polityka bezpieczeństwa odnosi się całościowo do problemu zabezpieczenia danych osobowych przetwarzanych w systemach informatycznych. Mając świadomość, aby reguły zabezpieczenia były znane wszystkim pracownikom Starostwa opracowano ten dokument.

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Starostwie Powiatowym w Wałbrzychu z wyłączeniem systemów „POJAZD" i KIEROWCA" użytkowanych w Wydziale Komunikacji i Transportu. Instrukcje dla tych systemów zostały opracowane przez PWPW w Warszawie (administratora systemu).

„Polityka bezpieczeństwa" obowiązuje wszystkich pracowników Starostwa Powiatowego w Wałbrzychu.

Intencją Starosty Wałbrzyskiego – Administratora Danych jest kompleksowe zabezpieczenie danych osobowych w tym celu: powołał Administratora Bezpieczeństwa Informacji, który odpowiedzialny jest za realizację zadań i za przestrzeganie zapisów zawartych w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. 2002 r. Nr 101 poz. 926 z późn. zm.) i rozporządzeniu Ministra Spraw Wewnętrznych Administracji z dnia 29 kwietnia 2004 r. (Dz. U. Nr 100 poz. 1024) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych – w zakresie ochrony danych osobowych.

Na szczeblu Wydziału za bezpieczeństwo i ochronę danych osobowych jak również za zapewnienie ciągłego i niezakłóconego funkcjonowania systemu odpowiada Naczelnik Wydziału. Natomiast na stanowisku pracy, pracownik, który posiada odpowiednie upoważnienie Administratora Danych do przetwarzania danych osobowych w systemie informatycznym.

Polityka bezpieczeństwa odnosi się do ochrony wszystkich zbiorów danych osobowych, które podlegają zgłoszeniu do rejestracji do Generalnego Inspektora Ochrony Danych Osobowych jak

również zbiorów, które nie podlegają rejestracji, a w których przetwarza się dane osób zatrudnionych w Starostwie.

Celem polityki bezpieczeństwa jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych w zakresie ochrony danych osobowych, sposobu przetwarzania danych osobowych, zabezpieczenie danych przetwarzanych w systemie informatycznym jak również ochrony sprzętu komputerowego służącego do przetwarzania tych informacji.

Bezpieczeństwo informacji – to bezpieczeństwo informacji, która jest przez system gromadzona i przetwarzana. System powinien, zgodnie z wymaganiami zapewnić poufność, integralność i dostępność informacji, a także autentyczność, niezaprzeczalność i rejestrowanie wykonywanych w nim operacji.

Zadaniem polityki bezpieczeństwa jest zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Główne zasady postępowania przy przetwarzaniu danych osobowych - każdy pracownik przetwarzający dane osobowe powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a co za tym idzie powinien przestrzegać pewnych zasad:

- ***zasada legalności*** – przetwarzać dane zgodnie z obowiązującym prawem;
- ***zasada celowości*** – zbierać dane dla oznaczonych, zgodnie z prawem celów i nie poddawać ich dalszemu przetwarzaniu niezgodnemu z tymi celami;
- ***zasady merytorycznej poprawności*** – dbać o merytoryczną poprawność danych;
- ***zasada adekwatności*** –przetwarzać tylko takiego rodzaju dane i tylko o takiej treści, które są niezbędne ze względu na cel zbierania danych. Relewantność (adekwatność) danych powinna być oceniania najpóźniej w momencie ich zbierania z uwzględnieniem określonego stosunku prawnego.
- ***zasady ograniczenia czasowego*** – przechowywać dane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

II. DEFINICJE

Ilekroć mowa w niniejszym dokumencie o:

1. **Administratorze danych osobowych** – należy przez to rozumieć osobę decydującą o celach i środkach przetwarzania danych osobowych – Starosta Wałbrzyski.
2. **Administratorze Bezpieczeństwa Informacji** – rozumie się przez to osobę powołaną zarządzeniem Starosty.
3. **Administratorze systemu** - rozumie się przez to informatyka lub osobę wyznaczoną do pełnienia tej funkcji przez administratora danych
4. **Danych osobowych** - rozumie się przez to wszelkie informacje dotyczące konkretnej osoby za pomocą, których bez większego wysiłku można tę osobę zidentyfikować, chociaż nie jest ona

wyraźnie wskazana. Do danych osobowych zalicza się nie tylko imię, nazwisko i adres osoby, ale również przypisane jej numery, dane o cechach fizjologicznych, umysłowych, ekonomicznych, kulturowych i społecznych. Danymi osobowymi nie są pojedyncze informacje o dużym stopniu ogólności, np. sama nazwa ulicy, czy wysokość wynagrodzenia.

5. **Zbiorze danych osobowych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

6. **Przetwarzaniu danych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie (nawet, jeśli faktycznie z nich się nie korzysta), opracowywanie, zmienianie, udostępnianie i usuwanie w systemie informatycznym.

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

8. **Zabezpieczeniu danych w systemie informatycznym** – należy przez to rozumieć zespół stosowanych środków technicznych i fizycznych w celu zabezpieczenia zasobów oraz ochrony danych przed ujawnieniem, zniszczeniem, utratą, a także nieuprawnionym dostępem i przetwarzaniem.

9. **Usuwaniu danych w systemie informatycznym** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą. W systemie informatycznym nośniki zawierające dane osobowe należy pozbawić na trwale zapisów tych danych, a w przypadku, gdy nie jest to możliwe, uszkodzić w sposób uniemożliwiający ich odczytanie np. spalenie, rozdrobnienie lub połamanie. Każdorazowo z faktu zniszczenia nośników zawierających dane osobowe należy sporządzić odpowiedni protokół.

10. **Udostępnianiu** – dane udostępniane są na zasadach ogólnych. Przepisy szczególne i unormowania zawarte w art. 23 i 27 ustawy o ochronie danych osobowych są wystarczającą podstawą umożliwiającą dostęp do danych osobowych. Gdy jest to niezbędne do realizacji przepisów prawa, zawierania umowy, gdy osoba, której dane dotyczą jest jej stroną, wykonywania zadań dla dobra publicznego (np. powódź, klęska), usprawiedliwionych celów realizowanych przez administratora danych osobowych (marketing własnych produktów, dochodzenie roszczeń z tytułu prowadzonej działalności). Osoba zwracająca się o dane musi też wyraźnie określić, jakich danych żąda i do jakiego celu zamierza je wykorzystać.

    W przypadku danych należących do kategorii danych szczególnie chronionych, do których należą informacje o pochodzeniu rasowym lub etnicznym, poglądach politycznych, religijnych, filozoficznych, wyznaniu, przynależności do partii lub związku, stanie zdrowia, kodzie genetycznym, nałogach, życiu seksualnym, danych dotyczących skazań, orzeczeniach o ukaraniu, mandatach i innych orzeczeniach wydanych w postępowaniu przed sądem lub urzędem, dane te mogą być wykorzystywane wyłącznie zgodnie z celem, dla którego zostały zgromadzone. Gdy o dane te występuje pojedyncza osoba – można je udostępnić jedynie wtedy, gdy podmiot zwracający się o nie jest do tego upoważniony przez przepisy prawa. Jeśli takich przepisów nie ma, nie jest możliwe udostępnienie tych danych, chociażby osoba zwracająca się o nie jak

najbardziej uwiarygodniła potrzebę ich posiadania. Ocena należy do administratora danych osobowych.

11. **Identyfikatorze użytkownika (login)** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
12. **Haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
13. **Poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.
14. **Integralności danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
15. **Uwierzytelnianiu** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
16. **Osobie upoważnionej do przetwarzania danych osobowych** – rozumie się przez to osobę, która upoważniona została na piśmie przez Starostę do przetwarzania danych osobowych w systemie informatycznym;
17. **Użytkowniku** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych,

III. ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator danych osobowych realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza;
   1) upoważnia poszczególne osoby do przetwarzania danych osobowych w stosownym, indywidualnie określonym zakresie;
   2) wyznacza administratora bezpieczeństwa informacji oraz określa zakres jego zadań;
   3) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych;
   4) zleca administratorowi bezpieczeństwa informacji zapewnienie użytkownikom odpowiednich stanowisk pracy umożliwiających bezpieczne przetwarzanie danych;
   5) podejmuje decyzje o celach i środkach przetwarzania danych osobowych, zwłaszcza z uwzględnieniem zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych osobowych.
2. Administrator bezpieczeństwa informacji (ABI) w szczególności:
   1) sprawuje nadzór nad wdrożeniem stosownych środków organizacyjnych, technicznych i fizycznych w celu zapewnienia bezpieczeństwa danych;
   2) sprawuje nadzór nad funkcjonowaniem systemu zabezpieczeń, w tym także nad prowadzeniem ewidencji z zakresu ochrony danych osobowych;
   3) nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom;
   4) przygotowuje wnioski zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych oraz prowadzi inną korespondencje z Generalnym Inspektorem;

5) zatwierdza wzory dokumentów dotyczących ochrony danych osobowych przygotowywane przez komórki organizacyjne;
6) prowadzi ewidencję i inną dokumentację z zakresu ochrony danych osobowych;
7) prowadzi oraz aktualizuje dokumentacje opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych;
8) podejmuje odpowiednie działania w wypadku naruszenia systemu informatycznego;
9) występuje z wnioskiem do administratora systemu o nadanie identyfikatora i przyznanie hasła osobie upoważnionej do przetwarzania danych osobowych;
10) przygotowuje wyciągi z polityki bezpieczeństwa dostosowane do zakresów obowiązków osób upoważnianych do przetwarzania danych osobowych;
11) przygotowuje materiały szkoleniowe z zakresu ochrony danych osobowych i prowadzi szkolenia osób upoważnianych do przetwarzania danych osobowych;
12) w porozumieniu z administratorem danych osobowych na czas nieobecności (urlop, choroba) wyznacza swojego zastępcę.

3. Administrator systemu w szczególności:
   1) zarządza systemem informatycznym, w którym przetwarzane są dane osobowe;
   2) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe;
   3) na wniosek administratora bezpieczeństwa informacji, przydziela każdemu użytkownikowi identyfikator i hasło do systemu informatycznego oraz na polecenie administratora danych dokonuje ewentualnych modyfikacji uprawnień;
   4) nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;
   5) podejmuje działania w zakresie ustalenia i kontroli identyfikatorów dostępu do systemu informatycznego;
   6) wyrejestrowuje użytkowników na wniosek administratora danych lub administratora bezpieczeństwa informacji;
   7) zmienia w poszczególnych stacjach roboczych hasła dostępu, ujawniając je wyłącznie danemu użytkownikowi oraz w razie potrzeby administratorowi bezpieczeństwa informacji lub administratorowi danych;
   8) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje ABI o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia;
   9) prowadzi szczegółową dokumentacje naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym;
   10) nadzoruje wykonywanie napraw, konserwacje oraz likwidację urządzeń komputerowych, na których zapisane są dane osobowe, sprawuje nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego;

11) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

4. Osoba upoważniona do przetwarzania danych osobowych może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez administratora danych i tylko w celu wykonywania nałożonych na niego obowiązków. Zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika niezbędnego do rozpoczęcia pracy w systemie. Rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych.
5. Użytkownicy danych pisemnie oświadczają, że zobowiązują się do zachowania tajemnicy danych osobowych oraz przestrzegania procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u administratora danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji.
6. Naruszenie przez użytkowników danych osobowych procedur bezpiecznego przetwarzania tych danych, w szczególności świadome udostępnienie danych osobie niepowołanej, jest ciężkim naruszeniem obowiązków pracowniczych.
7. Wszyscy użytkownicy danych zobowiązują się do:
   1) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych, w tym przepisami niniejszej polityki i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
   2) stosowania określonych przez administratora danych oraz administratora bezpieczeństwa informacji procedur oraz wytycznych mających na celu zgodne z prawem, w tym zwłaszcza adekwatne przetwarzanie danych;
   3) odpowiedniego zabezpieczenia danych przed ich udostępnianiem osobom nieupoważnionym.

IV. INFRASTRUKTURA PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator danych przetwarza dane osobowe w budynku przy al. Wyzwolenia 20-24 w Wałbrzychu. Obszar przetwarzania danych osobowych obejmuje wykaz wydziałów i samodzielnych stanowisk, w których są przetwarzane dane osobowe:
   1) Wydział Geodezji, Kartografii i Gospodarki Nieruchomościami
   2) Wydział Administracji Architektoniczno-Budowlanej
   3) Wydział Ochrony Środowiska
   4) Wydział Komunikacji i Transportu
   5) Wydział Organizacyjny i Spraw Obywatelskich
   6) Wydział Edukacji, Promocji i Rozwoju
   7) Wydział Infrastruktury Powiatu
   8) Wydział Finansowy
   9) Biuro Rady
   10) Powiatowy Rzecznik Konsumentów

11) Stanowisko ds. Zarządzania Ruchem na Drogach
12) Stanowisko ds. BHP

2. Wykaz pomieszczeń, w których przetwarzane są dane osobowe w systemie informatycznym oraz opis systemów informatycznych i ich zabezpieczeń zawiera **załącznik nr 1** do niniejszego dokumentu.
3. Wykaz zbiorów danych osobowych przetwarzanych przez administratora danych jest następujący:
   - dokumentacja papierowa (korespondencja, wnioski, deklaracje itd.),
   - urządzenia i oprogramowanie komputerowe służące do przetwarzania informacji oraz procedury przetwarzania danych w tym systemie, w tym procedury awaryjne,
   - wydruki komputerowe,
4. Wykaz zbiorów danych osobowych przetwarzanych w systemie informatycznym prowadzi Administrator Bezpieczeństwa Informacji – zgodnie z **załącznikiem nr 2**
5. Administrator Bezpieczeństwa Informacji prowadzi: ewidencję osób upoważnionych do przetwarzania danych osobowych.
6. Administrator Bezpieczeństwa Informacji prowadzi ewidencję udostępnień danych odbiorcom danych oraz innym podmiotom.
7. Administrator systemu prowadzi przechowywaną w kasie pancernej ewidencję haseł administracyjnych.

V. STRUKTURA ZBIORU DANYCH OSOBOWYCH

Opis struktur zbiorów danych osobowych oraz powiązań między zbiorami jak również sposób przepływu danych pomiędzy poszczególnymi systemami prowadzi Administrator Bezpieczeństwa Informacji.

VI. STRATEGIA ZABEZPIECZENIA DANYCH OSOBOWYCH (DZIAŁANIA NIEZBĘDNE DO ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH)

1. Administrator danych, zgodnie z ustawą z 21 listopada 2008r. o pracownikach samorządowych Dz. U. Nr 223, poz. 1458), prowadzi nabór na stanowiska urzędnicze w drodze konkursu. Jednym z kryteriów oceny kandydatów jest przedstawienie przez nich oświadczenia o niekaralności wszyscy pracownicy są dobierani z uwzględnieniem ich kompetencji merytorycznych, a także kwalifikacji moralnych. Zwraca się uwagę na takie cechy kandydata, jak: uczciwość, odpowiedzialność, przewidywalność zachowań.
2. W siedzibie administratora danych wydzielono strefę bezpieczeństwa klasy I, w której dostęp do informacji zabezpieczony jest wewnętrznymi środkami kontroli. Są to:
   - Pomieszczenia z serwerami, w których może przebywać wyłącznie informatyk oraz inne osoby mające upoważnienie administratora danych do przebywania w serwerowniach, osoby

postronne w ogóle nie mają dostępu; osoby mające wstęp do serwerowni maja określone PIN-y i karty.

- Pomieszczenie archiwum, w którym może przebywać tylko archiwista oraz osoba, której zlecono porządkowanie archiwum, inne osoby upoważnione do przetwarzania danych osobowych tylko w towarzystwie archiwisty, osoby postronne w ogóle nie mają dostępu; złożony w Wydziale Organizacyjnym i Spraw Obywatelskich klucz jest zabezpieczony i opisany;

3. W strefie bezpieczeństwa klasy II do danych osobowych mają dostęp wszystkie osoby upoważnione do przetwarzania danych osobowych zgodnie z zakresami upoważnień do przetwarzania danych osobowych, a osoby postronne tylko w obecności pracownika upoważnionego do przetwarzania danych osobowych. Strefa ta obejmuje wszystkie pozostałe pomieszczenia zaliczone do obszaru przetwarzania danych w siedzibie administratora danych. Do strefy bezpieczeństwa klasy II należy także Biuro Obsługi Klienta. Jednak przeglądanie akt spraw i sporządzanie z nich notatek przez strony jest możliwe tylko w obecności pracownika upoważnionego do przetwarzania danych osobowych.
4. Serwery są zlokalizowane w odrębnych, klimatyzowanych pomieszczeniach zamykanych antywłamaniowymi drzwiami. Okna do tych pomieszczeń zabezpieczone są szybami antywłamaniowymi, które spełniają normy zabezpieczenia przed włamaniem. W pomieszczeniach zamontowano instalację alarmową (czujniki ruchu podłączone do centrum monitorowania alarmów), drzwi zamykane są na zamki patentowe. Zastosowano oznakowanie pomieszczeń („zakaz wstępu osobom nieupoważnionym"). Na korytarzu zainstalowano monitoring wizyjny.
5. Większość urządzeń systemu informatycznego administratora danych jest zasilana za pośrednictwem zasilaczy awaryjnych (tzw. UPS-ów).
6. Sieć lokalna podłączona do Internetu oddzielona jest sprzętowym firewallem.
7. Bieżąca konserwacja sprzętu wykorzystywanego przez administratora danych do ich przetwarzania prowadzona jest tylko przez jego pracowników, przede wszystkim przez Informatyka. Natomiast poważne naprawy wykonane przez personel zewnętrzny realizowane są w siedzibie administratora danych po zawarciu z podmiotem wykonującym naprawę umowy o powierzenie przetwarzania danych osobowych, określającej kary umowne za naruszenie bezpieczeństwa danych.
8. Wszystkie awarie, działania konserwacyjne i naprawy systemu informatycznego są opisywane w stosownych protokołach podpisywanych przez osoby w nich uczestniczące, a także przez administratora bezpieczeństwa informacji.
9. Administrator systemu dopuszcza konserwowanie i naprawę sprzętu poza siedzibą administratora danych jedynie po trwałym usunięciu danych osobowych. Zużyty sprzęt służący do przetwarzania danych osobowych może być zbywany dopiero po trwałym usunięciu danych osobowych, a urządzenia uszkodzone powinny być przekazywane właściwym podmiotom w celu utylizacji. Zawiera się z nimi umowy powierzenia przetwarzania danych.
10. Administrator systemu, administrator bezpieczeństwa Informacji wskazuje użytkownikom, jak postępować, aby zapewnić:

1) ochronę elektromagnetyczną nośników danych – dyskietek z danymi, a szczególnie nośników danych, na których przechowywane są kopie zapasowe (należy przechowywać je z dala od magnesów oraz urządzeń wytwarzających pole magnetyczne, a więc nie wprost na urządzeniach komputerowych),
2) prawidłową lokalizację komputerów.

12. Niezwykle ważne dla bezpieczeństwa danych jest wyrobienie przez każdą osobę upoważnioną do przetwarzania danych lub użytkownika nawyku:

1) kasowania po wykorzystaniu danych na dyskach przenośnych;
2) nie używania powtórnie jednostronnie zadrukowanych dokumentów;
3) zachowanie tajemnicy danych, w tym także wobec najbliższych;
4) pilnego strzeżenia akt, dyskietek, pamięci przenośnych i komputerów przenośnych;
5) nie pozostawiania bez kontroli dokumentów, nośników danych i sprzętu w hotelach i innych miejscach publicznych ani też w samochodach;
6) ustawiania ekranów komputerowych tak, aby osoby nie powołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia;
7) nie zapisywania hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku;
8) nie podłączania do listew podtrzymujących napięcie, przeznaczonych dla sprzętu komputerowego, innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejników, czajników, wentylatorów);
9) dbania o prawidłową wentylację komputerów (nie można zasłaniać im kratek wentylatorów meblami, zasłonami lub stawiać tuż przy ścianie);
10) powstrzymywania się przez osoby upoważnione do przetwarzania danych osobowych od samodzielnej integracji w oprogramowanie i konfiguracje powierzonego sprzętu (szczególnie komputerów przenośnych), nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych;
11) przestrzegania przez osoby upoważnione do przetwarzania danych osobowych swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń administratora bezpieczeństwa informacji;
12) nie pozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych;
13) opuszczania stanowiska pracy dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób;
14) kopiowanie tylko jednostkowych danych (pojedynczych plików), obowiązuje zakaz robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonania obowiązków przez pracownika; jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach; po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki na których są przechowywane;
15) udostępniania danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej;

16) nie wynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej;
17) wykonania kopii roboczych danych, na których się właśnie pracuje, tak często, aby zapobiec ich utratę;
18) kończenia pracy na stacji roboczej po wprowadzeniu danych przetwarzanych tego dnia w odpowiednie obszary serwera, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w UPS i listwie;
19) niszczenie w niszczarce lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe, przed opuszczeniem miejsca pracy po zakończeniu dnia pracy;
20) chowanie do zamykanych na klucz szaf wszelkich akt zawierających dane osobowe, przed opuszczeniem miejsca pracy po zakończeniu dnia pracy;
21) umieszczania kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy;
22) zamykania okien w razie opadów lub innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych;
23) zamykania okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy;
24) zamykania drzwi na klucz po zakończeniu pracy w danym dniu.

13. Jeśli niemożliwe jest umieszczenie wszystkich dokumentów zawierających dane osobowe w zamykanych szafach, to należy powiadomić o tym Sekretarza Powiatu lub naczelnika Wydziału Organizacyjnego, który zgłasza osobom sprzątającym jednorazową rezygnację z wykonania usługi sprzątania.

14. Osoby upoważnione do przetwarzania danych osobowych powinny pamiętać zwłaszcza, że:

1) dane z nośników po wprowadzeniu ich do systemu informatycznego administratora danych powinny być trwale usuwane z tych nośników przez fizyczne zniszczenie (np. płyty CD-ROM) lub skasowanie danych programem usuwającym trwale pliki; jeśli istnieje uzasadniona konieczność, to dane pojedynczych osób (a nie całe zbiory czy obszerne wypisy ze zbiorów) mogą być przechowywane na specjalnie oznaczonych nośnikach; nośniki te muszą być przechowywane w zamkniętych na klucz szafach, nie mogą być udostępniane osobom postronnym; po ustaniu przydatności tych danych nośniki powinny być trwale kasowane lub niszczone;
2) uszkodzone nośniki przed ich wyrzuceniem należy zniszczyć fizycznie (przeciąć, przełamać);
3) po wykorzystaniu wydruki zawierające dane osobowe należy codziennie przed zakończeniem pracy zniszczyć w niszczarce; jeżeli to możliwe, nie należy przechowywać takich wydruków na biurku ani wynosić poza siedzibę administratora danych;
4) zabrania się powtórnego używania do sporządzania brudnopisów pism jednostronnie zadrukowanych kart, jeśli zawierają one chronione dane; zaleca się natomiast dwustronne drukowanie brudnopisów pism i sporządzanie dwustronnych dokumentów.

15. Bezpieczeństwo danych, a w szczególności ich integralność i dostępność w dużym stopniu zależy od zdyscyplinowanego, codziennego umieszczania danych w wyznaczonych zasobach serwera. Pozwala to przynajmniej w pewnym stopniu – uniknąć wielokrotnego wprowadzania tych samych danych do systemu informatycznego administratora danych. Sporządzanie kopii zapasowych

określa „Instrukcja zarządzania systemem informatyczny służącym do przetwarzania danych osobowych".

16. Inne wymogi bezpieczeństwa systemowego określają instrukcje obsługi producentów sprzętu i używanych programów, wskazówki administratora bezpieczeństwa informacji oraz „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

17. Pocztą elektroniczną (miedzy komputerami przenośnymi, a stacjonarnymi systemu informatycznego administratora danych) można przesyłać tylko jednostkowe dane, a nie całe bazy lub obszerne z nich wypisy, i tylko w postaci zaszyfrowanej. Chroni to przesłane dane przed „przesłuchami" na liniach teletransmisyjnych oraz przed przypadkowym rozproszeniem ich w internecie.

18. Przed atakami z sieci zewnętrznej wszystkie komputery administratora danych (w tym także przenośne) chronione są środkami dobranymi przez administratora systemu w porozumieniu z administratorem bezpieczeństwa informacji. Ważne jest, aby użytkownicy zwracali uwagę na to, czy urządzenie, na którym pracują, domaga się aktualizacji tych zabezpieczeń. O wszystkich takich przypadkach należy informować administratora bezpieczeństwa informacji lub informatyka oraz umożliwić im monitorowanie oraz aktualizację środków (urządzeń, programów) bezpieczeństwa.

19. Administrator systemu w porozumieniu z administratorem bezpieczeństwa informacji dobiera elektronicznie środki ochrony przed atakami z sieci stosownie do pojawiania się nowych zagrożeń (nowe wirusy, robaki, trojany, inne możliwości wdarcia się do systemu), a także stosownie do rozbudowy systemu informatycznego administratora danych i powiększania bazy danych. Jednocześnie należy zwracać uwagę czy rozwijający się system zabezpieczeń sam nie powoduje nowych zagrożeń.

20. Stosuje się następujące sposoby kryptograficzne ochrony danych:

1) przy przesyłaniu danych za pomocą poczty elektronicznej stosuje się protokół POP – tunelowanie;
2) przy przesyłaniu danych pracowników, niezbędnych do wykonania przelewów wynagrodzeń, używa się bezpiecznych stron https://.

21. Poszczególnym osobom upoważnionym do przetwarzania danych osobowych przydziela się konta opatrzone niepowtarzalnym identyfikatorem umożliwiające dostęp do danych, zgodnie z zakresem upoważnienia do przetwarzania danych osobowych. Administrator systemu, po uprzednim przedłożeniu upoważnienia do przetwarzania danych osobowych, przydziela pracownikowi upoważnionemu do przetwarzania danych konto w systemie informatycznym dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem.

22. W razie potrzeby, po uzyskaniu uprzedniej akceptacji administratora bezpieczeństwa informacji, administrator systemu może przydzielić konto opatrzone identyfikatorem osobie upoważnionej do przetwarzania danych osobowych nie mającej statusu pracownika.

23. Pierwsze hasło wymagane do uwierzytelnienia się w systemie przydzielane jest przez administratora systemu po odebraniu od osoby upoważnionej do przetwarzania danych oświadczenia zawierającego zobowiązanie do zachowania w tajemnicy pierwszego i następnych haseł oraz odbioru pierwszego hasła.

24. Do zagwarantowania poufności i integralności danych osobowych konieczne jest przestrzeganie przez użytkowników swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowanie się do zaleceń administratora bezpieczeństwa informacji i informatyka.

25. System informatyczny posiada szerokopasmowe połączenie z internetem. Dostęp do niego jest jednak ograniczony. Przyłączone są tylko wybrane stacje robocze.

26. Korzystanie z zasobów sieci wewnętrznej (intranet) jest możliwe tylko w zakresie uprawnień przypisanych do danego konta osoby upoważnionej do przetwarzania danych osobowych.

27. Urządzenia przenośne oraz nośniki danych wynoszone z siedziby administratora danych – Starostwa nie powinny być pozostawiane bez nadzoru w miejscach publicznych. Komputery przenośne należy przewozić w służbowych torbach. Wykorzystywanie własnych charakterystycznych toreb na laptopy nie jest dopuszczalne.

28. Nie należy pozostawiać bez kontroli dokumentów, nośników danych i sprzętu w hotelach i innych miejscach publicznych ani samochodach.

29. Informacje przechowywane na urządzeniach przenośnych lub komputerowych nośnikach danych należy chronić przed uszkodzeniami fizycznymi, a także uszkodzeniami wynikającymi z działania silnego pola elektromagnetycznego. Należy przestrzegać zaleceń producentów dotyczących ochrony sprzętu.

30. Wykorzystywanie komputerów przenośnych administratora danych w miejscach publicznych jest dozwolone, jeżeli otoczenie, w którym znajduje się osoba upoważniona do przetwarzania danych osobowych, stwarza warunki minimalizujące ryzyko zapoznania się z danymi przez osoby nieupoważnione. W konsekwencji korzystanie z komputera przenośnego jest niedozwolone w restauracjach czy środkach komunikacji publicznej.

31. W domu natomiast niedozwolone jest udostępnianie domownikom komputera przenośnego należącego do administratora danych. Użytkownik powinien zachować w tajemnicy wobec domowników identyfikator i hasło, których podanie jest koniecznie do rozpoczęcia pracy na komputerze przenośnym administratora danych.

32. Administrator systemu w razie potrzeby wskazuje w dokumencie powierzenia komputera przenośnego osobie upoważnionej do przetwarzania danych osobowych na konieczność i częstotliwość sporządzania kopii zapasowych danych przetwarzanych na komputerze przenośnym administratora danych oraz określa zasady:

1) postępowania w razie nieobecności w pracy dłużej niż 5 dni. Jeśli komputer przenośny nie może być zwrócony przed okresem nieobecności, to użytkownik tego komputera powinien niezwłocznie powiadomić o tym administratora bezpieczeństwa informacji i uzgodnić z nim zwrot komputera przenośnego administratorowi danych;
2) zwrotu sprzętu w razie zakończenia pracy u administratora danych.

33. W zakresie nieuregulowanym w polityce bezpieczeństwa do pracy z wykorzystaniem komputerów przenośnych stosuje się postanowienia ,,Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

34. Administrator systemu przeprowadza synchronizację zegarów stacji roboczych z serwerem, ograniczając dopuszczalność zmiany w ustawieniach zegarów. Jakiekolwiek zmiany ustawień zegarów mogą być dokonywane jedynie przez informatyka z konta o uprawnieniach administracyjnych.

35. System informatyczny administratora danych umożliwia zapisywanie zdarzeń wyjątkowych na potrzeby audytu i przechowywanie informacji o nich przez określony czas.

36. Zapisy takie obejmują:

1) identyfikator użytkownika;
2) datę i czas zalogowania i wylogowania się systemu;
3) tożsamość stacji roboczej;
4) zapisy udanych i nieudanych prób dostępu do systemu,
5) zapisy udanych i nieudanych prób dostępu do danych osobowych i innych zasobów systemowych.

37. Administrator bezpieczeństwa informacji przeprowadza raz w roku przegląd przetwarzanych danych osobowych pod kątem celowości ich dalszego przetwarzania. Osoby upoważnione do przetwarzania danych osobowych, w tym zwłaszcza naczelnicy poszczególnych wydziałów, są zobowiązani współpracować z administratorem bezpieczeństwa informacji w tym zakresie przez wypełnienie kwestionariuszy przeglądu i w razie potrzeby udzielenie innych koniecznych informacji.

38. Administrator bezpieczeństwa informacji może zarządzić przeprowadzenie dodatkowego przeglądu w wyżej określonym zakresie w razie zmian w obowiązującym prawie, ograniczających dopuszczalny zakres przetwarzanych danych osobowych. Dodatkowy przegląd może być konieczny także w sytuacji zmian organizacyjnych administratora danych.

39. Z przebiegu usuwania danych osobowych należy sporządzić protokół podpisywany przez administratora bezpieczeństwa informacji i naczelnika wydziału, w którym usunięto dane osobowe.

40. Wykazy zbiorów danych osobowych przechowywane są zgodnie z zapisami Rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U. Nr 14 poz. 67) i przechowywane w archiwum zakładowym zgodnie z Jednolitym Rzeczowym Wykazem Akt stanowiącym załącznik do ww. Rozporządzenia.

41. Administrator bezpieczeństwa informacji prowadzi plan szkoleń. Zgodnie z planem szkoli się każdą osobę, która ma zostać upoważniona do przetwarzania danych osobowych. Szkolenia wewnętrzne wszystkich osób upoważnionych do przetwarzania danych osobowych przeprowadzane są w wypadku każdej zmiany zasad lub procedur ochrony danych osobowych.

42. Tematyka szkoleń obejmuje:

1) przepisy i instrukcje dotyczące ochrony danych osobowych, sporządzania i przechowywania ich kopii, niszczenia wydruków i zapisów na nośnikach,
2) sposoby ochrony danych przed osobami postronnymi i procedury udostępniania danych osobom, których one dotyczą,
3) obowiązki osób upoważnionych do przetwarzania danych osobowych,
4) zasady i procedury określone w polityce bezpieczeństwa.

43. Niezastosowanie się do prowadzonej przez administratora danych polityki bezpieczeństwa przetwarzania danych osobowych, której założenia określa niniejszy dokument, naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowanie, jako ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym, w szczególności wynikającym z art. 51-54 ustawy oraz art. 266 Kodeksu Karnego.

44. Polityka bezpieczeństwa powinna być poddawana przeglądowi przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych administrator bezpieczeństwa informacji może zarządzić przegląd polityki bezpieczeństwa stosownie do potrzeb.

45. Administrator bezpieczeństwa informacji analizuje, czy polityka bezpieczeństwa i pozostała dokumentacja jest adekwatna do zmian:

1) w budowie systemu informatycznego,
2) zmian organizacyjnych Administratora danych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,
3) zmian w obowiązującym prawie.

46. Administrator bezpieczeństwa informacji po uzgodnieniu ze Starostą może stosownie do potrzeb, przeprowadzić audyt systemu informatycznego. Przeprowadzenie audytu wymaga uzgodnienia jego zakresu z administratorem systemu. Zakres, przebieg i rezultaty audytu udokumentowane są na piśmie w protokole podpisywanym zarówno przez administratora bezpieczeństwa informacji, jak i informatyka.

47. Starosta w razie konieczności może zlecić przeprowadzenie audytu zewnętrznego przez wyspecjalizowany podmiot.

VII. POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. W przypadku stwierdzenia naruszenia:
   1) zabezpieczenie systemu informatycznego,
   2) technicznego stanu urządzeń,
   3) zawartości zbioru danych osobowych,
   4) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
   5) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, kradzież zbiorów danych, rejestrów, itp.)

Każda osoba jest zobowiązana do niezwłocznego powiadomienia o tym fakcie administratora bezpieczeństwa informacji i bezpośredniego przełożonego.

2. Po wykonaniu czynności określonych w ust.1 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 i sprawców,
2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,

Jednym z podstawowych działań powinno być nie podawanie swojego adresu e – mailowego bez potrzeby innym oraz w formie niezabezpieczonej na stronie WWW i na grupach dyskusyjnych. Jeżeli na witrynach wymagane jest podanie adresu poczty elektronicznej uważnie należy przeczytać jakie obowiązują na niej zasady prywatności, do czego ten adres może zostać użyty. Nie należy odpowiadać na listy od spamerów, nie należy wchodzić na żadne linki wysyłane w wiadomościach od nieznanych nadawców. W programie pocztowym należy korzystać z filtrów. Natomiast w przypadku uciążliwego spamu, należy zgłosić to do administratora serwera.

- Jak zabezpieczyć się przed phishingiem?

Phishing to wiadomość, która zachęca do kliknięcia umieszczonego w niej odnośnika, przenosząc nas na fałszywą stronę jakiejś organizacji (najczęściej są to banki). Tam proszeni jesteśmy o podanie swoich danych osobowych lub pobranie jakiegoś oprogramowania, które okazuje się być trojanem (wirusem komputerowym, najczęściej prostym programem komputerowym, który w sposób celowy powiela się bez zgody użytkownika).

Cechami charakterystycznymi dla tego rodzaju wiadomości są:

- masowe ich przesyłanie pocztą elektroniczną lub za pośrednictwem komunikatorów internetowych,
- zachęcanie użytkownika do kliknięcia linku przekierowującego na określoną witrynę, na której musi wprowadzić poufne dane, aby np. dokonać ich potwierdzenia lub ponownie aktywować konto,
- alarmowy charakter takich wiadomości, ostrzegający przed atakiem (w wiadomości często zawarta jest informacja, że ze względów bezpieczeństwa użytkownicy powinni odwiedzić witrynę www i potwierdzić swoje dane: nazwę użytkownika, hasło, numer karty kredytowej, numer PIN, numer PESEL itp.).

Aby ochronić się przed tym zagrożeniem należy zawsze dokładnie sprawdzić, czy dana strona internetowa lub e-mail są godne zaufania. Ignorować e-maile wzywające do wprowadzenia danych potrzebnych do logowania, nawet, jeżeli ich autorzy grożą zablokowaniem konta i podobnymi konsekwencjami. Żadna poważna instytucja nie żąda nigdy podania swoich danych lub ich aktualizacji tą drogą. Jeżeli chcemy mieć całkowitą pewność powinniśmy zadzwonić i osobiście dowiedzieć się czy e-mail faktycznie pochodzi od danej instytucji. Atak może być skierowany na konkretną instytucję, w którym phisher wyświetla zapytanie dotyczące szczegółów pracownika, które umożliwiają uzyskanie dostępu do reszty sieci.

W Starostwie Powiatowym w Wałbrzychu w celu zabezpieczenia sieci zastosowano ochronę przed wirusami, spamami polegającą na zainstalowaniu programów antywirusowych na serwerze i w poszczególnych komputerach, filtru antyspamowego na serwerze, którego zadaniem jest, aby wiadomości rozpoznane, jako spam nie docierały do skrzynek pocztowych. Oprócz zabezpieczeń programowych, każdy pracownik powinien przestrzegać pewnych zasad:

- nie pracować na koncie administratora,
- nie ściągać z Internetu programów i materiałów,
- nie używać jednego hasła do wszystkich kont,
- nie odpowiadać na „dziwne' e-maile niezwiązane z charakterem pracy.

Niezależnie od rodzaju zagrożenia mogą to być *zagrożenia* wewnętrzne lub zewnętrzne.

Zagrożenia losowe wewnętrzne:

3) zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę zdarzenia,
4) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego lub aplikacji użytkowej,
5) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
6) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia administratora bezpieczeństwa informacji lub osoby upoważnionej.

3. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, administrator bezpieczeństwa informacji lub osoba upoważniona:
1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Starostwa,
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) w razie potrzeby powiadamia o zaistniałym naruszeniu Starostę,
4) jeżeli zachodzi taka potrzeba zleca usunięcie występujących naruszeń oraz powiadamia odpowiednie instytucje.
4. Administrator bezpieczeństwa informacji dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego załącznik nr 3.
5. Raport, o którym mowa w ust. 4, Administrator bezpieczeństwa informacji niezwłocznie przekazuje Administratorowi danych osobowych, a w przypadku jego nieobecności osobie uprawnionej.
6. Zaistniałe naruszenie może stać się przedmiotem szczegółowej analizy prowadzonej przez zespół powołany przez Starostę.
7. Analiza, o której mowa w ust.6, 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.

VIII. KLASYFIKACJA ZAGROŻEŃ SYSTEMÓW KOMPUTEROWYCH

Systemy komputerowe są połączeniem sprzętu oraz pracującego na nim oprogramowania. W zależności od czynnika powodującego powstanie zagrożenia systemu komputerowego dzielony jest na sprzętowe oraz programowe. *Zagrożenia sprzętowe* powodowane są fizycznie przez sprzęt komputerowy (np. awaria urządzenia), natomiast *zagrożenia programowe* spowodowane są przez oprogramowanie komputerów (np. błąd programu).

Niezależnie od czynnika powodującego zagrożenie może być ono przypadkowe lub celowe.

1. Zagrożenie przypadkowe jest wtedy, kiedy powstało samoczynnie (np. awaria sprzętu, błąd oprogramowania) lub nieumyślnie (błąd ludzki, np. roztargnienie, posiadanie niewystarczającej na dany temat wiedzy). Tego typu zagrożenia nie dają się z góry przewidzieć, ale można im przeciwdziałać i zmniejszać szanse ich wystąpienia (np. dublowanie urządzeń, nieużywanie wersji testowych oprogramowania, szkolenie pracowników).
2. Zagrożenie celowe powstaje w wyniku świadomej ingerencji ludzi w sprzęt lub oprogramowanie, mające na celu zniszczenie, przechwycenie bądź modyfikację systemu komputerowego. Przeciwdziałać temu zagrożeniu można jedynie poprzez jak największe utrudnienia w dostępie do

systemu nieupoważnionym osobom, nadzorowanie zachowania osób upoważnionych do korzystania z systemu oraz podnoszenia świadomości bezpieczeństwa komputerowego wśród użytkowników np. szkolenia. Każdy komputer musi być zabezpieczony hasłem uruchomieniowym składającym się z 8 znaków tj. z liter i cyfr. Do zagrożeń celowych należy zaliczyć również działania hakerów, crakerów, spamy i pfishing, który jest zagrożeniem polegającym na wykradaniu od użytkowników Internetu danych osobowych, haseł dostępu, loginów itp.

- Jak zabezpieczyć się przed hakerami i crakerami?

  Generalnie hakerzy koncentrują się na łamaniu zabezpieczeń systemów teleinformatycznych po to, aby wykazać możliwość zmieniania treści przetwarzanych danych oraz uzyskiwania do nich dostępu. Ich działania mają na celu przede wszystkim informowanie administratorów i producentów oprogramowania o wykrytych lukach, a często również informowanie opinii publicznej o dokonaniu ataku dla podkreślenia własnych umiejętności i zdobycia w ten sposób uznania w środowisku. Działania hakerów rzadko mają na celu wyrządzenie szkody instytucjom lub osobom, których dane są przetwarzane, ale wyniki ich pracy mogą być wykorzystane przez inne osoby – crakerów w celach typowo przestępczych.

  Crakerzy z kolei to osoby, które stosując dostępne w sieci narzędzia programowe, wykorzystują je w celach przestępczych, np. do przechwycenia uprawnień dostępu do cudzego konta w systemie informatycznym banku, operatora telefonicznego itp. w celu wykonania na swoją korzyść określonych działań lub pozyskania cennych informacji, np. projektów chronionych prawem autorskim, tajemnicą przedsiębiorstwa bądź innych danych chronionych, jak np. dane osobowe. W zależności od celu i skuteczności ataku, wyrządzone szkody mogą mieć charakter czysto ekonomiczny (np. kradzież środków finansowych), szpiegowski (np. kradzież informacji, m.in. handlowej, naukowo-technicznej, technologicznej, organizacyjnej itp.), a także społeczny (utrata zaufania, reputacji). W literaturze nie zawsze rozróżnia się wymienione typy działań i obydwie grupy osób zalicza się do tzw. cyberprzestępców.

  Nie ma 100% zabezpieczenia przed tymi grupami, jednakże utrudnieniem dla potencjalnych ataków może okazać się zainstalowanie Firewall (zapory sieciowej). Crakerzy często dokonują włamań i pozyskują różnego rodzaju hasła poprzez stworzone przez siebie wirusy, dlatego też niezbędne jest wyposażenie sprzętu komputerowego w skuteczny program antywirusowy. Ważne jest, aby nie zapisywać na dysku ważnych danych dotyczących np. haseł do kont bankowych, numerów haseł dostępu do systemów informatycznych. Hasła zabezpieczające powinny składać się z małych i dużych liter, cyfr i znaków specjalnych. Zabezpieczeniem może również okazać się nie podpinanie pod sprzęt komputerowy różnego rodzaju nośników danych nieznanego pochodzenia.

- Jak zabezpieczyć się przed spamem?

  Spam (niechciana lub niepotrzebna wiadomość elektroniczna, najczęściej rozpowszechniana za pośrednictwem poczty elektronicznej). Aby określić wiadomość mianem spamu, musi spełnić trzy następujące warunki jednocześnie:

  1. Treść wiadomości jest niezależna od tożsamości odbiorcy.
  2. Odbiorca nie wyraził uprzedniej, zamierzonej zgody na otrzymanie tej wiadomości.
  3. Treść wiadomości daje podstawę do przypuszczeń, że nadawca wskutek jej wysłania może odnieść zyski nieproporcjonalne w stosunku do korzyści odbiorcy.

- Błędnie skonfigurowane systemy operacyjne i programy. Błędy popełnione podczas konfiguracji systemu mogą znacząco wpłynąć na jego poziom bezpieczeństwa.
- Błędy w oprogramowaniu. W każdym oprogramowaniu można znaleźć błędy, co może zostać wykorzystane do naruszenia bezpieczeństwa danych.
- Błędy i zaniedbania użytkowników. Upoważnieni użytkownicy z powodu niewiedzy lub zmęczenia popełniają błędy, dokonują niecelowych zniszczeń sprzętu bądź danych.
- Rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia, w którym znajdują się dane osobowe, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.)
- Losowe uszkodzenie sprzętu. Naturalne uszkodzenia elementów systemu, np. wskutek wad fabrycznych, zmęczenia materiału itp.

Zagrożenia losowe zewnętrzne:

- Nieodpowiednia temperatura lub wilgotność powietrza w pomieszczeniach, w których umieszczone są elementy systemu informatycznego – eliminacja tego zagrożenia polega na zmianie pomieszczenia, zastosowania odpowiedniego systemu ogrzewania lub klimatyzacji.
- Zanieczyszczenie powietrza – eliminacja zagrożenia polega na odpowiedniej wentylacji pomieszczeń.
- Zakłócenia bądź przerwy w dostawie zasilania – zabezpieczeniem przed tym zagrożeniem jest zastosowanie urządzeń podtrzymujących zasilanie „UPS".
- Wyładowania atmosferyczne – budynek zabezpieczony odgromnikami.
- Klęski żywiołowe takie, jak:
  - pożar – w celu minimalizacji skutków tego zagrożenia założona jest sieć czujników dymu na korytarzach i w pokojach, na korytarzach zamontowane są hydranty. Dodatkowo w pokojach, w których przetwarzane się dane osobowe w systemie informatycznych znajdują się gaśnice przeciwpożarowe.
  - powódź – pomieszczenia biurowe, w których przetwarzane są dane osobowe w przypadku wystąpienia powodzi nie są narażone na zalanie wodą.
- Włamanie – przeciwdziałanie polega na prawidłowym zabezpieczeniu okien i drzwi oraz zamontowaniu w pomieszczeniach czujników ruchu. Na parterze w budynku przy al. Wyzwolenia 24 (Wydział Komunikacji i Transportu) zamontowano monitoring wizyjny, który nadzoruje pracownik ochrony.
- Kradzieże – w celu wyeliminowania tego zagrożenia należy pamiętać o zamykaniu na klucz pokoju na czas nieobecności pracowników. Wychodząc z pracy należy dokumenty i nośniki informacji zabezpieczyć w szafach zamykanych na klucz.

Zagrożenia zewnętrzne możliwe są do przewidzenia i można się do nich odpowiednio przygotować i je wyeliminować, natomiast wewnętrzne są zazwyczaj niespodziewane i przez to szczególnie niebezpieczne.

Załącznik nr 1

Wykaz pomieszczeń, w których przetwarzane są dane osobowe w Starostwie i ich zabezpieczeń.

1. Wykaz pomieszczeń, w których przetwarzane są dane osobowe.

Lp.	Nazwa komórki	Lokalizacja	Nr pokoju

2. W celu ochrony przed utratą danych w Starostwie stosowane są następujące zabezpieczenia:
   1) odrębne zasilanie sprzętu komputerowego oraz zastosowanie zasilaczy awaryjnych UPS,
   2) ochrona serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy awaryjnych UPS,
   3) ochrona przed utratą zgromadzonych danych przez robienie kopii zapasowych na płytach CD, CDRW, DVD, z których w przypadku awarii odtwarzane są dane.
   4) pomieszczenia biurowe lub inne w których przechowywane są zbiory danych osobowych zamykane są na zamki patentowe, posiadają zabezpieczenie przeciwpożarowe (pomieszczenia na parterze wyposażone są w okna antywłamaniowe).
   5) kopie zapasowe zbiorów danych osobowych przechowywane są w zamykanych na klucz szafach, do których klucze posiadają tylko upoważnieni pracownicy.
3. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Starostwa:

   1) aby uzyskać dostęp do zasobów sieci, należy zwrócić się do Administratora Bezpieczeństwa Informacji z odpowiednim wnioskiem w którym podane będą dane nowego użytkownika oraz zasoby jakie ma on mieć udostępnione.

   2) w systemie informatycznym Urzędu zastosowano podwójną autoryzację użytkownika. Pierwszej autoryzacji należy dokonać w momencie uzyskania dostępu do systemu operacyjnego Starostwa, podając login użytkownika i hasło; drugiej autoryzacji należy dokonać uruchamiając program użytkowy, podając login użytkownika i hasło; dostęp do wybranej bazy danych Starostwa uzyskuje się dopiero po poprawnym podwójnym zalogowaniu się do systemu informatycznego Starostwa.

4. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Starostwa poprzez internet.

W zakresie dostępu z sieci wewnętrznej Starostwa do sieci rozległej Internet zastosowano firewall, który ma za zadanie uwierzytelnianie źródła przychodzących wiadomości oraz filtrowanie pakietów w oparciu o adres IP, numer portu i inne parametry. Ściana ogniowa składa się z bezpiecznego systemu operacyjnego i filtra pakietów. Ruch pakietów, który firewall przepuszcza jest określony przez administratora.

Firewall zapisuje do logu fakt zaistnienia wyjątkowych zdarzeń i śledzi ruch pakietów przechodzących przez nią. Dostęp do sieci jest ustalony indywidualnie dla każdego użytkownika na podstawie wniosku.

Oprócz filtra pakietów (firewall) zastosowano również system wykrywający obecność wirusów w poczcie elektronicznej.

W efekcie zapewnione jest:

1) zabezpieczenie sieci przed atakiem z zewnątrz poprzez blokowanie wybranych portów,
2) filtrowanie pakietów i blokowanie niektórych usług,
3) objęcie ochroną antywirusową wszystkich danych ściąganych z internetu na stacjach lokalnych,

5. Postanowienia końcowe.

1) do pomieszczeń w których następuje przetwarzanie danych osobowych mają dostęp tylko uprawnione osoby bezpośrednio związane z nadzorem nad serwerami lub aplikacjami,
2) zabezpieczenie przed nieuprawnionym dostępem do danych, prowadzone jest przez Administratora Bezpieczeństwa Informacji zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego,
3) osoby mające dostęp do danych powinny posiadać zaświadczenie o przebytym szkoleniu z zakresu ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r.
4) w pomieszczeniach w których znajdują się serwery jest zamontowana klimatyzacja, która zapewnia właściwą temperaturę i wilgotność powietrza dla sprzętu komputerowego
5) większość urządzeń w serwerowni umieszczona jest w szafach serwerowych i sieciowych.

Załącznik nr 2

Nazwa Wydziału / komórki organizacyjnej

Lp.	Nazwa zbioru	Rodzaj zbioru	Podlega rejestracji w GIODO/ nie podlega

Zestawienie zbiorcze

Lp.	Nazwa wydziału	Ilość zarejestrowanych zbiorów	Ilość podlegających zgłoszeniu	Ilość zbiorów	Rodzaj zbioru

Załącznik nr 3

Raport

z naruszenia bezpieczeństwa systemu informatycznego

w Starostwie Powiatowym w Wałbrzychu

1. Data:.....godzina:.....
(dd.mm.rrrr) *(00:00)*

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....

(Imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje))

1.Lokalizacja zdarzenia:

.....

(np. nr pokoju, nazwa pomieszczenia)

2. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....

.....

3. Podjęte działania:

.....

.....

4. Przyczyny wystąpienia zdarzenia:

.....

.....

5. Postępowanie wyjaśniające:

.....

.....

.....

data, podpis Administratora Bezpieczeństwa Informacji

Zakończenie

Dokument pn. „Polityka Bezpieczeństwa Przetwarzania Danych Osobowych w Systemie Informatycznym w Starostwie Powiatowym w Wałbrzychu" stanowi wewnętrzny dokument Starostwa Powiatowego w Wałbrzychu, zostaje przekazany drogą elektroniczną do wszystkich Wydziałów Starostwa Powiatowego w Wałbrzychu. Naczelnicy Wydziałów odpowiadają za zakomunikowanie „Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Systemie Informatycznym w Starostwie Powiatowym w Wałbrzychu " pracownikom i egzekwowanie przestrzegania jej zapisów w pracy przez pracowników związanych z przetwarzaniem danych osobowych i ich ochroną.

STAROSTA
Józef Piksa