Zarządzenie Nr 35/12
Starosty Stargardzkiego
z dnia 12 marca 2012 r.

w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Starostwie Powiatowym w Stargardzie Szczecińskim

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. 2002 r. Nr 101 poz. 926 z późn. zm.), § 3 i 4 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 (Dz. U. Nr 100, poz. 1024) oraz § 6 ust 1 pkt 8 Uchwały Nr III/35/10 Rady Powiatu w Stargardzie Szczecińskim z dnia 29 grudnia 2010 r. w sprawie uchwalenia Regulaminu Organizacyjnego Starostwa Powiatowego w Stargardzie Szczecińskim zarządzam, co następuje:

Polityka bezpieczeństwa informacji
w Starostwie Powiatowym w Stargardzie Szczecińskim

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych oraz w systemach nieinformatycznych w Starostwie Powiatowym w Stargardzie Szczecińskim. Opisane reguły określają granice dopuszczalnego przetwarzania danych osobowych, zwracają uwagę na konsekwencje jakie mogą ponosić osoby przekraczające określone granice oraz wskazują procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Potrzeba opracowania dokumentu „Polityka Bezpieczeństwa Informacji" zwanego dalej „Polityka Bezpieczeństwa" wynika z § 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).

Rozdział I
Postanowienia Ogólne

§1

Określenia i skróty użyte w Polityce oznaczają:

1) Administrator Danych Osobowych – Starosta Stargardzki, zwany dalej Administratorem,
2) Administrator Bezpieczeństwa Informacji, zwany dalej ABI – osoba wyznaczona przez Administratora, w rozumieniu art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101 poz. 926 z późn. zm.), dalej jako Ustawa,

3) Administrator Systemów Informatycznych, zwani dalej ASI – pracownik wyznaczony, odpowiedzialny za wdrażanie i stosowanie zasad bezpieczeństwa danych osobowych w zakresie technicznych zabezpieczeń systemu informatycznego w urzędzie,
4) Osoba upoważniona, zwana dalej użytkownikiem – osoba posiadająca upoważnienie nadane przez Administratora lub osobę wyznaczoną przez niego i uprawniona do przetwarzania danych osobowych, w zakresie wskazanym w upoważnieniu,
5) System informatyczny, zwany dalej systemem, w rozumieniu art. 7 pkt 2a) Ustawy,
6) Zabezpieczenie danych w systemie, zwane dalej zabezpieczeniem – czynności wykonywane w rozumieniu art. 7 pkt 2b) Ustawy,
7) Starostwo Powiatowe w Stargardzie Szczecińskim zwane dalej starostwem.

§ 2

1. Polityka określa podstawowe zasady przetwarzania danych osobowych, określa ich granice oraz wskazuje procedury jakie należy stosować w przypadku ich przekroczenia.
2. Polityka dotyczy wszystkich danych osobowych, przetwarzanych w starostwie, niezależnie od formy ich przetwarzania (papierowe zbiory ewidencyjne, systemy informatyczne) oraz od tego czy dane są lub mogą być przetwarzane w zbiorach danych.
3. Polityka ma zastosowanie wobec wszystkich komórek organizacyjnych starostwa.
4. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych osobowych przetwarzanych w starostwie.
5. Administrator danych, którym jest Starosta Stargardzki, swoją decyzją wyznacza Administratora Bezpieczeństwa Informacji danych osobowych przetwarzanych w starostwie, zwanego dalej "ABI".
6. ABI realizuje zadania w zakresie ochrony danych osobowych wynikające z ustawy oraz z aktów wewnętrznych starostwa.

§ 3

1. Celem Polityki jest ochrona danych osobowych, przetwarzanych w urzędzie przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz ich ochrona przed zmianą, uszkodzeniem lub zniszczeniem.
2. Cele Polityki realizowane są poprzez zapewnienie danym osobowym następujących cech:
   1) poufności — właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom;
   2) integralności — właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   3) rozliczalności — właściwości zapewniającej, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
3. Za podmiot nieupoważniony uważa się podmiot, który nie otrzymał zgody Administratora na udostępnienie mu danych osobowych w trybie i na zasadach określonych w ustawie o ochronie danych osobowych oraz osobę nieposiadającą

upoważnienia do przetwarzania danych osobowych, nadanego przez Administratora w trybie art. 37 Ustawy.

4. Niniejszy dokument jest zgodny z następującymi aktami prawnymi:
   1) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.),
   2) ustawą o ochronie informacji niejawnych z dnia 22 stycznia 1999 r. (Dz. U. Nr 11, poz. 95 z późn. zm.),
   3) rozporządzeniem Prezesa Rady Ministrów z dnia 25 sierpnia 2005 roku w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 171, poz. 1433),
   4) rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji - do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz. U. Nr 100, poz. 1023).

Rozdział II
Opis zdarzeń naruszających ochronę danych osobowych

§4

1. Podział zagrożeń:
   1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych,
   2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych,
   3) zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony dostęp do danych osobowych z zewnątrz (włamanie , w tym włamanie do systemu informatycznego), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych nośników danych osobowych.
2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia bezpieczeństwa przetwarzania danych osobowych to głównie:
   1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na nośniki danych osobowych jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
   2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,

3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
6) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.,
12) podmieniono lub zniszczono wszelkie nośniki z danymi osobowymi ,bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,
13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero lub innych niezabezpieczonych miejscach, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.

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

Rozdział III
Zabezpieczenie danych osobowych

§5

1. Administratorem danych osobowych zawartych i przetwarzanych w systemach informatycznych starostwa jest Starosta.
2. Administrator jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych starostwa, a w szczególności:
   1) zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
   2) zapobiegać przed zabraniem danych przez osobę nieuprawnioną,

3) zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

3. Stosuje się następujące środki techniczne :
   1) budynek urzędu przy ul. Skarbowej 1 ,zamykany po zakończeniu pracy, jest nadzorowany przez :
      - pracownika dozoru w godz. od 6.00 do 22.00 w dni robocze a w dni wolne od pracy całą dobę.
      - przez system alarmowy; w dni robocze od 22.00 do 6.00 godz. a w dni wolne od pracy cała dobę,
   2) pomieszczenia urzędu w budynku przy ul. Bogusława IV 21, zabezpieczone są zamkami patentowymi, wejście do budynku jest zabezpieczone kodem,
   3) pomieszczenia urzędu, w których są przetwarzane dane osobowe są zabezpieczone zamkami patentowymi oraz posiadają system alarmowy,
   4) wyposażenie ww. pomieszczeń w szafy i szafki z zamkami dającymi gwarancję bezpieczeństwa dokumentacji zawierającej dane osobowe,
   5) zapewniające identyfikacje osób mających dostęp do obszarów przetwarzanie danych podczas nieobecności osób upoważnionych do przetwarzania danych
   6) urządzenia wchodzące w skład systemu informatycznego połączone są do odrębnego obwodu elektrycznego, zabezpieczonego na wypadek zaniku napięcia albo awarii w sieci zasilającej ups-em,
   7) sieć lokalna podłączona do Internetu oddzielona jest sprzętowym firewallem,
   8) na serwerze oraz w poszczególnych stacjach roboczych zainstalowano oprogramowanie antywirusowe,
   9) regularne tworzenie kopii zapasowych baz danych aplikacji, w której przetwarzane są dane osobowe,
   10) komputery, z których możliwy jest dostęp do danych osobowych zabezpieczone są hasłem wejściowym do systemu operacyjnego oraz hasłem do każdej aplikacji przy pomocy, której przetwarzane są dane osobowe,
   11) dla każdego użytkownika systemu ustalony jest odrębny identyfikator,
   12) dane transferowane na zewnątrz przez program Płatnik zabezpieczone są połączeniem szyfrowanym.
4. Stosuje się następujące środki organizacyjne:
   1) zapoznanie każdego pracownika z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych,
   2) nadanie każdemu pracownikowi przetwarzającemu dane osobowe stosownego upoważnienia oraz prowadzenie ewidencji osób upoważnionych
   3) kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane osobowe, poprzez wprowadzenie polityki zarządzania kluczami, która stanowi Załącznik nr 4 do Polityki Bezpieczeństwa Informacji,
   4) wprowadzenie instrukcji zarządzania systemem informatycznym,
   5) wprowadzenie procedur postępowania w przypadku naruszenia danych osobowych.

5. Dane wrażliwe należy przechowywać w zamykanych pomieszczeniach w szafkach zamykanych na klucz. Nie udostępniać podmiotom zewnętrznym.

§6

1. Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka dla poszczególnych systemów, stosuje się następujące poziomy bezpieczeństwa:
   a) podstawowy,
   b) podwyższony,
   c) wysoki.
2. Określenia poziomu bezpieczeństwa systemu informatycznego dokonuje ABI
3. Poziomy bezpieczeństwa odnotowuje się w dokumentacji prowadzonej w przez ABI
4. Niezależnie od niniejszych zasad opisanych w dokumencie „Polityka bezpieczeństwa" w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie.

Rozdział IV
Wykaz budynków i pomieszczeń, w których przetwarzane są dane osobowe

§7

Wykaz budynków i pomieszczeń w których przetwarzane są dane osobowe załącznik nr 1 do niniejszego dokumentu.

Rozdział V
Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

§8

1. Zbiory danych osobowych są przetwarzane w sposób tradycyjny bez użycia systemu informatycznego(ewidencje, rejestry) a część z nich także poprzez określone aplikacje systemu informatycznego.
2. Wykaz zbiorów danych oraz programów zastosowanych do przetwarzania tych danych określony jest w załączniki nr 2 do niniejszego dokumentu.

Rozdział VI
Opis struktury zbiorów danych oraz sposób przepływu danych pomiędzy systemami

§9

1. Dane osobowe są przetwarzane przy zastosowaniu systemów informatycznych, w zbiorach ewidencyjnych oraz poza zbiorami.

2. Zbiory danych osobowych zlokalizowane są w przedmiotowych bazach danych umieszczonych na serwerze.
3. Dane osobowe w zbiorach są przetwarzane tylko w aplikacjach (programach) dostosowanych do merytorycznych potrzeb komórek organizacyjnych starostwa.
4. Zawartość pól informacyjnych, występujących w aplikacjach (programach) systemów zastosowanych do przetwarzania danych, musi być zgodna z przepisami prawa, które uprawniają lub zobowiązują Administratora do przetwarzania danych osobowych.
5. Opis struktury zbiorów oraz opis przepływu danych pomiędzy systemami stanowi załącznik nr 3 do niniejszego dokumentu.

Rozdział VII
Kontrola przestrzegania zasad zabezpieczenia danych osobowych

§10

1. Administrator lub osoba przez niego wyznaczona, którą jest ABI sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.
2. ABI w porozumieniu z ASI sporządza roczny plan kontroli zatwierdzony przez Starostę i zgodnie z nim przeprowadza kontrole oraz dokonuje oceny stanu bezpieczeństwa danych osobowych.
3. Na podstawie zgromadzonych materiałów, o których mowa w ust. 2, ABI sporządza roczne sprawozdanie i przedstawia Administratorowi do końca stycznia każdego roku.

Rozdział VIII
Postępowanie w przypadku naruszenia danych osobowych

§11

1. W przypadku stwierdzenia naruszenia:
   1) zabezpieczenia systemu informatycznego,
   2) technicznego stanu urządzeń,
   3) zawartości zbioru danych osobowych,
   4) ujawnienia metody pracy lub sposobu działania programu,
   5) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
   6) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.)

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

2. W razie niemożliwości zawiadomienia ABI lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego.
3. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych ABI lub upoważnionej przez niego osoby, należy:
   1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie

uwzględnić w działaniu również ustalenie przyczyn lub sprawców,

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

4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, ABI lub osoba go zastępująca:
   1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy 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) rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora danych .
   4) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza starostwa.
5. ABI dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego załącznik nr 5, który powinien zawierać w szczególności:
   1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
   2) określenie czasu i miejsca naruszenia i powiadomienia,
   3) określenie okoliczności towarzyszących i rodzaju naruszenia,
   4) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
   5) wstępną ocenę przyczyn wystąpienia naruszenia,
   6) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.
6. Raport, o którym mowa w ust. 6, ABI niezwłocznie przekazuje Administratorowi, a w przypadku jego nieobecności Sekretarzowi Powiatu.
7. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu ABI zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

8. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Członków Zarządu, Sekretarza Powiatu, ABI, Pełnomocnika ds. Ochrony Informacji Niejawnych, Wydział Audytu i Kontroli.
9. Analiza, o której mowa w ust. 9, powinna zawierać wszechstronną ocenę zaistniałego naruszenia,
wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Rozdział IX
Postanowienia końcowe

§12

1. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym zarządzeniu, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
2. ABI zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych.
3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym ABI.
4. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia ABI nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
5. W sprawach nie uregulowanych niniejszym zarządzeniem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji - do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz. U. Nr 100, poz. 1023).

§13

Traci moc Zarządzenie Nr 47/05 Starosty Stargardzkiego z dnia 28 grudnia 2005 r. w sprawie ustalenia polityki bezpieczeństwa danych osobowych oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Stargardzie Szczecińskim.

§14

Zarządzenie wchodzi w życie z dniem podpisania.

Starosta

Waldemar Gil

Załącznik nr 1 do Polityki Bezpieczeństwa

Obszary przetwarzania danych w pomieszczeniach budynku przy ul. Skarbowej 1

poziom -1

Nr pokoju	Komórka organizacyjna
002	Biuro Obsługi Urzędu

parter

Nr pokoju	Komórka organizacyjna
05,06,	Biuro Zamówień
07,08, 09	Wydział Spraw Społecznych i Zdrowia
10,11,12,	Wydział Komunikacji
02,03, kancelaria	Biuro Obsługi Urzędu

I piętro- lewe skrzydło budynku

Nr pokoju	Komórka organizacyjna
104,106,107,108. 114	Biuro Obsługi Zarządu i Rady Powiatu
101, 205,	Wydział Środowiska

I piętro- prawe skrzydło budynku

Nr pokoju	Komórka organizacyjna
116,118,	Wydział Kultury i Promocji Powiatu

II piętro- lewe skrzydło budynku budynku

Nr pokoju	Komórka organizacyjna
206,207,210, 211	Wydział Geodezji i Gospodarki Nieruchomościami

II piętro- prawe skrzydło

Nr pokoju	Komórka organizacyjna
220,	Powiatowy Rzecznik Konsumentów
221,222,223,224,	Wydział Urbanistyki, Architektury i Budownictwa

212,216, 04	Wydział Oświaty i Sportu
213,214,	Wydział Planowania i Rozwoju

III piętro- prawe skrzydło budynku

Nr pokoju	Komórka organizacyjna
304,305,306,307,308,	Wydział Finansowy

Obszary przetwarzania danych w pomieszczeniach budynku przy ul. Rynek staromiejski 5

Nr pokoju	Komórka organizacyjna
125,127	Wydział Geodezji i Gospodarki Nieruchomościami

Obszary przetwarzania danych w pomieszczeniach budynku przy ul. Bogusława IV 21

Nr pokoju	Komórka organizacyjna
215,218	Wydział Zarządzania Bezpieczeństwem
216,217,	Wydział Audytu i Kontroli

Starosta
Waldemar Gil

Załącznik nr 2 do Polityki Bezpieczeństwa

Wykaz zbiorów danych osobowych oraz programy zastosowane do przetwarzania tych danych

Zbiór osób pobierających świad. pieniężne	Kadry-Płace „Personal 88"
Zbiór osób zgłaszanych do ubezp. społecznego	Płatnik
Opłaty Skarbu Państwa	POWIAT INFORMIX
Zbór uczniów i studentów benef. projektów	Baza w formie pliku tekstowego - pEFS
Ewidencja właścicieli pojazdów	Centralna Ewidencja Pojazdów (CEP)
Ewidencja kierowców	Centralna Ewidencja Kierowców (CEK)
Ewidencja gruntów i budynków	Mienie
Rejestr Strażników Społecznej Straży Rybackiej Powiatu Stargardzkiego	Dane przetwarzane w tradycyjny sposób
Rejestr sprzętu pływającego do połowu ryb	Baza w formie pliku tekstowego
Rejestr wydanych kart wędkarskich	Baza w formie pliku tekstowego
Rejestr posiadaczy żywych zwierząt gatunków wymienionych w załącznikach Ai B rozporządzenia Rady(WE) 333/97 z dnia 9 grudnia 1996 r.	Dane przetwarzane w tradycyjny sposób
Rejestr decyzji i wniosków w sprawie wycięcia drzew i krzewów	Dane przetwarzane w tradycyjny sposób
Rejestr licencji wydawanych na krajowy transport osób i rzeczy	Dane przetwarzane w tradycyjny sposób oraz program „ Licencje Zezwolenia i Zaświadczenia na Przewóz Osób i Rzeczy"
Rejestr instruktorów nauki jazdy	Dane przetwarzane przez program „Instruktorzy nauki jazdy" oraz przetwarzane w tradycyjny sposób
Rejestr wydanych kart parkingowych	Dane przetwarzane w tradycyjny sposób
Rejestr imiennych uprawnień do wykonywania badań technicznych pojazdów	Dane przetwarzane w tradycyjny sposób
Rejestr przedsiębiorców prowadzących ośrodki szkolenia kierowców	Dane przetwarzane w tradycyjny sposób
Rejestr wniosków o wydanie zezwolenia na sprowadzenie zwłok	Dane przetwarzane w tradycyjny sposób
Rejestr rzeczy znalezionych	Dane przetwarzane w tradycyjny sposób
Zbiór wniosków konsumentów o udzielenie pomocy prawnej przez Powiatowego Rzecznika Konsumentów	Dane przetwarzane w tradycyjny sposób
Awans zawodowy nauczycieli	Dane przetwarzane w tradycyjny sposób
Rejestr szkół i placówek niepublicznych publicznych prowadzonych na terenie Powiatu Stargardzkiego	Dane przetwarzane w tradycyjny sposób

Rejestr osób skazanych odbywających karę prac społecznie użytecznych	Dane przetwarzane w tradycyjny sposób
Rejestr użytkowników wieczystych Skarbu Państwa	Dane przetwarzane w tradycyjny sposób
Rejestr właścicieli lasów nie stanowiących własności Skarbu Państwa	Dane przetwarzane w systemie informatycznym Geo-Info oraz przetwarzane w tradycyjny sposób
Skargi i wnioski	Dane przetwarzane w tradycyjny sposób
Kwalifikacja wojskowa	Dane przetwarzane w tradycyjny sposób
Rejestr pozwoleń na budowę	Dane przetwarzane w tradycyjny sposób
Rejestr zaświadczeń o samodzielności lokali	Dane przetwarzane w tradycyjny sposób
Ewidencja osób, którym zwrócono nieruchomości	Dane przetwarzane w tradycyjny sposób
Wykaz Radnych Rady Powiatu	Dane przetwarzane w tradycyjny sposób

Starosta

Waldemar Gil

Załącznik nr 3 do Polityki Bezpieczeństwa

Struktury zbiorów danych

Lp.	Zbiór danych	Struktura zbioru danych
1.		
	Osoby pobierające świadczenie pieniężne	Zbiór prowadzony w systemie informatycznym. Prowadzony jest w sposób centralny .Zawiera dane dotyczące osób fiz. pobierających świadczenie pieniężnae Zakres informacji gromadzonych w zbiorze: dane osobowe os. fiz.. obierających świadczenia pieniężne na podstawie stosunków prawnych łączących ich ze starostwem : nazwiska, imiona, imiona rodziców, data urodzenia, miejsce urodzenia, miejsce zamieszkania,(województwo, powiat, gmina, miejscowość ulica, nr domu) NIP, PESEL, nazwa wydziału, stanowisko, składniki wynagrodzenia, stopień niepełnosprawności, kod ubezpieczenia, dane osobowe dzieci (imie ,nazwisko, data urodzenia)
	Osoby zgłaszane do ubezpieczenia społecznego	Zbiór prowadzony w systemie informatycznym. Prowadzony jest w sposób centralny .Zawiera dane dotyczące osób fiz. zgłoszonych do ubezpieczenia społecznego. Zakres informacji gromadzonych w zbiorze: nazwiska, imiona, imiona rodziców, data urodzenia, miejsce urodzenia, miejsce zamieszkania,(województwo, powiat, gmina, miejscowość ulica, nr domu) NIP, PESEL
	Opłaty Skarbu Państwa	Zbiór prowadzony w systemie informatycznym. Prowadzony jest w sposób centralny .Zawiera dane dotyczące osób fiz. posiadających prawo użytkowania wieczystego. Zakres informacji gromadzonych w zbiorze: imię, nazwisko, adres zamieszkania,
	Centralna Ewidencja Pojazdów	Zbiór prowadzony w systemie informatycznym. Prowadzony jest w sposób centralny .Zawiera dane dotyczące osób fiz. będącymi właścicielami pojazdów. Zakres informacji gromadzonych w zbiorze: nazwiska i imiona, data urodzenia, miejsce urodzenia, adres zamieszkania, nr PESEL, nr i seria dow. osobistego, imiona rodziców, nr dow. rejestracyjnego, nr tablic rej.

	Centralna Ewidencja Kierowców	Zbiór prowadzony w systemie informatycznym. Prowadzony jest w sposób centralny .Zawiera dane dotyczące osób fiz. posiadających prawo jazdy. Zakres informacji gromadzonych w zbiorze: nazwiska i imiona,data urodzenia, miejsce urodzenia, adres zamieszkania, nr PESEL, nr i seria dow. osobistego, informacje dotyczące prawa jazdy, informacje dotyczące stanu zdrowia
	Ewidencja gruntów i budynków	Zbiór prowadzony w systemie informatycznym. Prowadzony jest w sposób centralny .Zawiera dane dotyczące osób fiz. bedących właścicielami gruntów i budynków. Zakres informacji gromadzonych w zbiorze: nazwiska i imiona, adres zamieszkania, nr PESEL
	Kwalifikacja wojskowa	Zbiór prowadzony po za systemem informatycznym. Prowadzony jest w sposób centralny .Dane gromadzone są od osób, których dotyczą. Zakres informacji gromadzonej w zbiorze Dane zgromadzone w zbiorze :osobowe: nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania, Nr książeczki wojskowej, kategoria zdolności, stan zdrowia,
	Skargi i wnioski	Zbiór prowadzony po za systemem informatycznym. Prowadzony jest w sposób centralny .Uporządkowany wg spisu spraw wpływających. Dane gromadzone są od osób, których dotyczą. Zakres informacji gromadzonych w zbiorze: dane osobowe osób składających wnioski i skargi : nazwiska i imiona, adres zamieszkania, nr telefonu
	Rejestr właścicieli lasów nie stanowiących własności Skarbu Państwa.	Zbiór prowadzony po za systemem informatycznym. Prowadzony jest w sposób centralny .Uporządkowany wg. spisu spraw wpływających. Dane gromadzone są od osób, których dotyczą. Zakres informacji gromadzonych w zbiorze : Dane osobowe właścicieli ww. lasów : nazwiska i imiona, miejsce zamieszkania, nr telefonu
	Rejestr użytkowników wieczystych Skarbu Państwa	Zbiór prowadzony w systemie informatycznym. Prowadzony jest w sposób centralny .Zawiera dane dotyczące osób fiz. posiadających prawo użytkowania wieczystego. Zakres informacji gromadzonych w zbiorze: nazwiska i imiona,

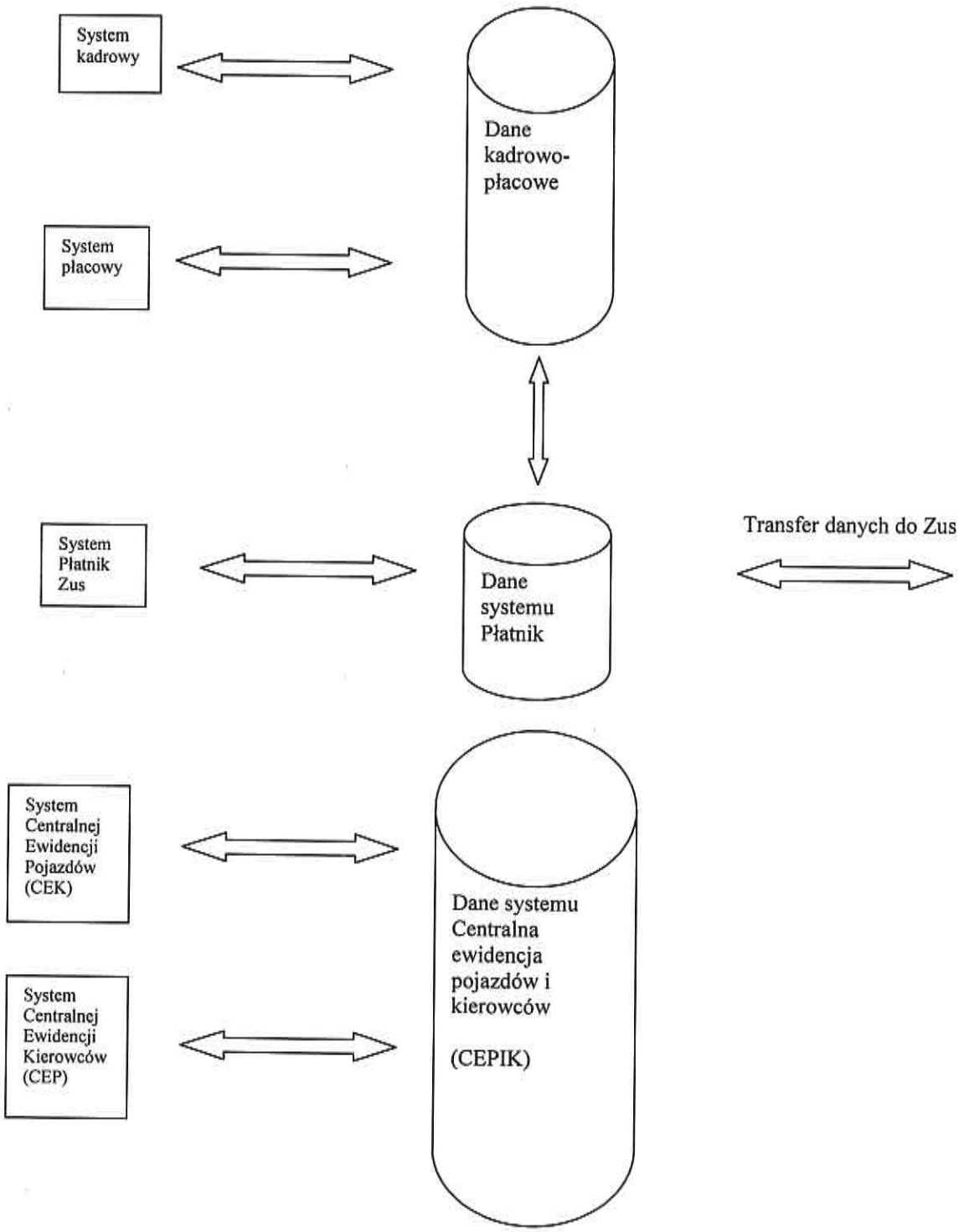
		imiona rodziców, adres zamieszkania lub pobytu, adres PESEL, NIP, seria i nr dow. osobistego
	Rejestr osób skazanych odbywających karę prac społecznie użytecznych.	Zbiór prowadzony po za systemem informatycznym. Prowadzony jest w sposób centralny .Uporządkowany wg spisu spraw wpływających. Dane pozyskiwane są ze źródeł zewnętrznych .Zakres informacji gromadzonych w zbiorze.: dane osobowe osób odbywających karę prac społecznie użytecznych : nazwiska i imiona, imiona rodziców, adres zamieszkania, data urodzenia, miejsce urodzenia, wymiar kary ograniczenia wolności,
	Rejestr szkół i placówek niepublicznych prowadzonych na terenie Powiatu Stargardzkiego	Zbiór prowadzony po za systemem informatycznym. Prowadzony jest w sposób centralny .Uporządkowany wg spisu spraw wpływających. Dane pozyskiwane są od osób, których dotyczą. Zakres informacji gromadzonych w zbiorze.: dane osób fizycznych prowadzących szkołę i placówkę niepubliczną oraz nauczycieli nazwiska i imiona, data urodzenia, miejsce urodzenia, adres zamieszkania, nr PESEL, miejsce pracy, zawód, wykształcenie, seria i nr dow. osobistego, nr telefonu
	Awans zawodowy nauczycieli	Zbiór prowadzony po za systemem informatycznym. Prowadzony jest w sposób centralny .Uporządkowany wg spisu spraw wpływających. Dane pozyskiwane są od osób, których dotyczą. Zakres informacji gromadzonych w zbiorze.: dane osobowe nauczycieli ubiegających się o awans zawodowy ; nazwiska i imiona, data urodzenia, miejsce urodzenia, adres zamieszkania, miejsce pracy, zawód, wykształcenie, seria i nr dow. osobistego
	Zbiór wniosków konsumentów o udzielenie pomocy prawnej przez Powiatowego Rzecznika Konsumentów	Zbiór prowadzony po za systemem informatycznym. Prowadzony jest w sposób centralny .Uporządkowany wg spisu spraw wpływających. Dane pozyskiwane są od osób, których dotyczą. Zakres informacji gromadzonych w zbiorze.: dane osobowe konsumentów ; nazwiska i imiona, adres zamieszkania, nr telefonu
	Rejestr wniosków o wydanie zezwolenia na sprowadzenie zwłok	Zbiór prowadzony po za systemem informatycznym. Prowadzony jest w sposób centralny .Uporządkowany wg spisu spraw wpływających. Dane pozyskiwane są od osób, których dotyczą. oraz z innych źródeł.

		Zakres informacji gromadzonych w zbiorze : dane osobowe osób składających wniosek o wydanie zezwolenia ; nazwiska, adres zamieszkania, nr telefonu,
	Rejestr Rzeczy Znalezionych	Zbiór prowadzony w systemie informatycznym i poza informatycznym. Prowadzony jest w sposób centralny. Uporządkowany wg spisu spraw wpływających. Dane pozyskiwane są od osób, których dotyczą..Zakres informacji gromadzonych w zbiorze : dane osobowe osób fizycznych zawiadamiających o odnalezieniu rzeczy oraz osoby upoważnione do jej odbioru ; nazwiska i imiona, adres zamieszkania, nr telefonu oraz opis przedmiotów wchodzących w skład rejestrów.
	Rejestr przedsiębiorców prowadzących ośrodki szkolenia kierowców	Zbiór prowadzony po za systemem informatycznym. Prowadzony jest w sposób centralny .Uporządkowany wg spisu spraw wpływających. Dane pozyskiwane są od osób, których dotyczą. oraz z innych źródeł. Zakres informacji gromadzonych w zbiorze : dane osobowe os. fizycznych prowadzących ośrodki szkolenia kierowców ; nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania, nr PESEL, NIP, wykształcenie, seria i nr dow. osobistego, oraz dane identyfikacyjne przedsiębiorcy oraz pojazdów będących własnością przedsiębiorcy.
	Rejestr imiennych uprawnień do wykonywania badań technicznych pojazdów.	Zbiór prowadzony po za systemem informatycznym. Prowadzony jest w sposób centralny .Uporządkowany wg spisu spraw wpływających. Dane pozyskiwane są od osób, których dotyczą oraz z innych źródeł. Zakres informacji gromadzonych w zbiorze : dane osobowe os. fizycznych ubiegających się o wydanie uprawnień diagnosty ; nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania, nr PESEL, wykształcenie, seria i nr dow. osobistego, nr telefonu
	Rejestr wydanych kart parkingowych	Zbiór prowadzony po za systemem informatycznym. Prowadzony jest w sposób centralny .Uporządkowany wg spisu spraw wpływających. Dane pozyskiwane są od osób, których dotyczą oraz z innych źródeł. .Zakres informacji gromadzonych w zbiorze : dane osobowe os. fiz. wnioskujących o

		wydanie kart parkingowych ; nazwiska i imiona, data urodzenia, adres zamieszkania, stan zdrowia
	Rejestr instruktorów nauki jazdy	Zbiór prowadzony w systemie informatycznym i pozainformatycznym. Prowadzony jest w sposób centralny. Uporządkowany wg spisu spraw wpływających. Dane pozyskiwane są od osób, których dotyczą oraz z innych źródeł.Zakres informacji gromadzonych w zbiorze : dane osobowe os. fiz. ubiegających się o wydanie legitymacji instruktora ; nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania, nr PESEL, NIP, wykształcenie, seria i nr dow. osobistego, stan zdrowia, dane o karalności,
	Rejestr licencji wydawany na krajowy transport	Zbiór prowadzony po za systemem informatycznym i pozainformatycznym. Prowadzony jest w sposób centralny. Uporządkowany wg spisu spraw wpływających. Dane pozyskiwane są od osób, których dotyczą. oraz z innych źródeł..Zakres informacji gromadzonych w zbiorze : dane osobowe os. fiz. prowadzących działalność w zakresie transportu ; nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania, nr PESEL, NIP, seria i nr dow. osobistego, dane o karalności a także inf. o stanie majątkowym, inf. dotycz. prowadzonej działalności, dane pojazdów znajdujących się w posiadaniu przedsiębiorcy
	Rejestr decyzji i wniosków w sprawie wycięcia drzew i krzewów.	Zbiór prowadzony po za systemem informatycznym. Prowadzony jest w sposób centralny. Uporządkowany wg spisu spraw wpływających. Dane pozyskiwane są od osób, których dotyczą. Zakres informacji gromadzonych w zbiorze : dane osobowe os. fiz. składających wniosek o wycięcie ; nazwiska i imiona, adres zamieszkania, nr telefonu, adres e-mail a także dane techniczne i formalne dotyczące gruntów,
	Rejestr posiadaczy żywych zwierząt gatunków wymienionych w załącznikach A i B rozporządzenia Rady (WE) nr 338/97 z dnia 9 grudnia 1996 r.	Zbiór prowadzony po za systemem informatycznym. Prowadzony jest w sposób centralny. Uporządkowany wg spisu spraw wpływających. Dane pozyskiwane są od osób, których dotyczą.Zakres informacji gromadzonych w zbiorze : dane osobowe

		os. fiz. występujących z wnioskami ; nazwiska i imiona, adres zamieszkania,
	Rejestr Strażników Społecznej Straży Rybackiej Powiatu Stargardzkiego	Zbiór prowadzony po za systemem informatycznym. Prowadzony jest w sposób centralny. Uporządkowany wg spisu spraw wpływających. Dane pozyskiwane są od osób, których dotyczą.Zakres informacji gromadzonych w zbiorze : dane osobowe os. fizycznych ubiegających się o wydanie legitymacji ; nazwiska i imiona, data urodzenia, adres zamieszkania
	Rejestr sprzętu pływającego do połowu ryb	Zbiór prowadzony po za systemem informatycznym. Prowadzony jest w sposób centralny. Uporządkowany wg spisu spraw wpływających. Dane pozyskiwane są od osób, których dotyczą...Zakres informacji gromadzonych w zbiorze : dane osobowe os. fiz. składających wniosek o rejestrację. ; nazwiska i imiona, miejsce zamieszkania.
	Rejestr wydanych kart wędkarskich	Zbiór prowadzony po za systemem informatycznym. Prowadzony jest w sposób centralny. Uporządkowany wg spisu spraw wpływających. Dane pozyskiwane są od osób, których dotyczą.Zakres informacji gromadzonych w zbiorze : dane osobowe os. fiz. , którym wydano karty wędkarskie: nazwiska i imiona, adres zamieszkania
	Wykaz Radnych Rady Powiatu	Zbiór prowadzony po za systemem informatycznym. Prowadzony jest w sposób centralny. Dane pozyskiwane są od osób, których dotyczą.Zakres informacji gromadzonych w zbiorze : dane osobowe Radnych Rady Powiatu; nazwiska i imiona, adres zamieszkania, data urodzenia, miejsce urodzenia, nr PESEL, NIP, miejsce pracy, zawód, wykształcenie, seria i nr dow. osobistego,

Starosta
Waldemar Gil



Starosta

Waldemar Gil

Załącznik nr 4 do
Polityki Bezpieczeństwa Informacji

Instrukcja zarządzania kluczami w Starostwie Powiatowym w Stargardzie Szczecińskim

§1 . Postanowienia ogólne

1. Niniejsza instrukcja reguluje sposób pobierania, zdawania i przechowywania kluczy do pomieszczeń w Starostwie Powiatowym w Stargardzie Szczecińskim.
2. Wszystkie klucze do pomieszczeń wraz z kluczami zapasowymi oznaczone są numerem i przechowywane w zamykanej na klucz szafce na recepcji.
3. Zabrania się zabierania kluczy po za teren obiektu za wyjątkiem określonym w pkt 4.
4. Przechowywanie kluczy przez użytkowników jest dopuszczalne wyłącznie za zgodą Sekretarza Powiatu na pisemny wniosek kierownika komórki organizacyjnej.
5. Ww. użytkownicy są obowiązani chronić klucz przed utratą, zniszczeniem oraz nieudostępnieniem osobom upoważnionym.
6. O utracie , uszkodzeniu lub zniszczeniu klucza użytkownik niezwłocznie powiadamia dyrektora Biura Obsługi Urzędu oraz ABI.

§ 2 . Tryb postępowania

1. Pracownik ochrony wydaje klucze do pomieszczeń po podpisaniu listy obecności przez pracownika.
2. Po zakończeniu pracy ww. pracownik ochrony sprawdza czy wszystkie klucze zostały zdane i odnotowuje ten fakt w książce ewidencji kluczy. W przypadku stwierdzenia nieoddania klucza pracownik ochrony zobowiązany jest bezzwłocznie do wyjaśnienia zaistniałego zdarzenia. W przypadku bezskuteczności podjętych działań ww. pracownik sprawdza zabezpieczenia pomieszczenia, sporządza notatkę z zaistniałego zdarzenia oraz powiadamia ABI.
3. W książce ewidencji należy odnotować również każdorazowy pobór klucza przez pracownika po godzinach pracy wskazując : imię i nazwisko pracownika datę i godzinę poboru oraz oddania oraz nr klucza.
4. Każdorazowe wydanie klucza zapasowego należy odnotować w książce ewidencji kluczy.
5. Wydawanie kluczy w dni świąteczne i wolne od pracy może nastąpić za zgodą Sekretarza Powiatu bądź Członka zarządu nadzorującego pracę danej komórki organizacyjnej. Pracownicy wykonujący pracę w dni świąteczne i wolne są zobowiązani do zgłoszenia na piśmie tego faktu pracownikom ochrony oraz podanie nazwisk osób upoważnionych do pobrania kluczy.

§ 3. Wydawanie kluczy sprzątaczkom

1. Tryb przyjmowania, przechowywania i wydawania kluczy sprzątaczkom:

a) klucze przydzielone sprzątaczkom są kluczami zapasowymi,

b) Wydanie i przyjęcie kluczy od sprzątaczki następuje po zarejestrowaniu tego faktu w książce ewidencji kluczy.

c) Pracownik ochrony sprawdza czy zdano wszystkie klucze. W przypadku stwierdzenia braku, bezzwłocznie do wyjaśnienia zaistniałego zdarzenia. W przypadku bezskuteczności podjętych działań ww. pracownik sprawdza zabezpieczenia pomieszczenia, sporządza notatkę z zaistniałego zdarzenia oraz powiadamia ABI.

§ 4. Postanowienia końcowe

1. W przypadkach nadzwyczajnych, kiedy pobór klucza, jest niezbędny dla zapewnienia bezpieczeństwa mienia znajdującego się w pomieszczeniach, pracownik ochrony bezzwłocznie wydaje klucz, odnotowując godzinę wydania i zdania, nr klucza oraz osobę, której został wydany.
2. Wszelkie naruszenia procedur opisanych w niniejszym dokumencie stanowi zdarzenie naruszające system ochrony danych osobowych wg. Polityki Bezpieczeństwa Informacji i może pociągać za sobą konsekwencje tam opisane.

STAROSTA

Waldemar Gil

Załącznik Nr 5
do Polityki Bezpieczeństwa Informacji

Raport z naruszenia bezpieczeństwa przetwarzania danych osobowych w Starostwie Powiatowym w Stargardzie Szczecińskim

1. Data :..... , godzina : .....
2. Osoba powiadamiająca o zaistniałym zdarzeniu : .....
3. Lokalizacja zdarzenia : .....
4. Rodzaj naruszenia:
   .....
   .....
   .....
5. Podjęte działania:
   .....
   .....
   .....
   .....
6. Przyczyny wystąpienia zdarzenia :
   .....
   .....
   .....
   .....
   .....
   .....
7. Postępowanie wyjaśniające:
   .....
   .....
   .....
   .....

Sporządził :
Administrator Bezpieczeństwa Informacji

Uwagi i zalecenia Administratora Danych Osobowych:

.....
.....
.....
.....
.....
.....
.....

.....
(data i podpis Administratora Danych Osobowych)

Starosta
Waldemar Gil