Zarządzenie Nr 136/17
Starosty Stargardzkiego
z dnia 5 grudnia 2017 roku

w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Starostwie Powiatowym w Stargardzie

Na podstawie art. 34 ust. 1 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2016 r. poz. 814 z późn. zm.), art. 36 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922 z późn. zm.), § 3 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) zarządza się, co następuje:

§ 1. W Starostwie Powiatowym w Stargardzie wprowadza się Politykę Bezpieczeństwa Informacji, stanowiącą załącznik do niniejszego zarządzenia.

§ 2. Zobowiązuje się wszystkich pracowników Starostwa Powiatowego w Stargardzie do zapoznania się z niniejszym zarządzeniem i załącznikami oraz do przestrzegania zasad zawartych w tych dokumentach. Oświadczenie o zapoznaniu się należy wpiąć do akt osobowych pracowników.

§ 3. Traci moc:
1) zarządzenie nr 52/10 Starosty Stargardzkiego z dnia 13 maja 2010 r. w sprawie zasad funkcjonowania sieci informatycznej Starostwa Powiatowego w Stargardzie Szczecińskim,
2) zarządzenie nr 35/12 Starosty Stargardzkiego z dnia 12 marca 2012 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Starostwie Powiatowym w Stargardzie Szczecińskim zmienione zarządzeniem 107/16 Starosty Stargardzkiego z dnia 22 lipca 2016 r.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA
Iwona Wiśniewska

Załącznik
do zarządzenia nr 136/17
Starosty Stargardzkiego
z dnia 5 grudnia 2017 roku

POLITYKA BEZPIECZEŃSTWA INFORMACJI STAROSTWA POWIATOWEGO w STARGARDZIE

Rozdział 1
Postanowienia ogólne, definicje i objaśnienia

§ 1.1. Polityka Bezpieczeństwa Informacji Starostwa Powiatowego w Stargardzie jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich zbiorach danych osobowych administrowanych przez Starostwo Powiatowe w Stargardzie.

2. Podstawą do opracowania i wdrożenia dokumentu są:
1) Konstytucja Rzeczypospolitej Polskiej;
2) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922 z późn. zm.);
3) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 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).

3. Polityka Bezpieczeństwa Informacji Starostwa Powiatowego w Stargardzie zawiera:
1) wykaz budynków i pomieszczeń, w których przetwarzane są dane osobowe, stanowiący załącznik nr 1 do niniejszej Polityki Bezpieczeństwa Informacji;
2) wykaz zbiorów danych osobowych przetwarzanych elektronicznie lub w inny sposób, stanowiący załącznik nr 2 do niniejszej Polityki Bezpieczeństwa Informacji;
3) opis struktury zbiorów danych osobowych przetwarzanych w systemach informatycznych oraz sposób przepływu danych pomiędzy systemami informatycznymi, stanowiący załącznik nr 3 do niniejszej Polityki Bezpieczeństwa Informacji;
4) instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, stanowiącą załącznik nr 4 Polityki Bezpieczeństwa Informacji;
5) instrukcję postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych, stanowiącą załącznik nr 5 do niniejszej Polityki Bezpieczeństwa Informacji;
6) wzór formularza zgody na przetwarzanie danych osobowych, stanowiącą załącznik nr 6 do niniejszej Polityki Bezpieczeństwa Informacji;
7) wzór formularza upoważnienia na przetwarzanie danych osobowych, stanowiącą załącznik nr 7 do niniejszej Polityki Bezpieczeństwa Informacji;
8) wzory oświadczeń osób upoważnionych do przetwarzania danych osobowych, stanowiącą załącznik nr 8 do niniejszej Polityki Bezpieczeństwa Informacji;
9) instrukcję zarządzania kluczami w Starostwie Powiatowym w Stargardzie, stanowiącą załącznik nr 9 do niniejszej Polityki Bezpieczeństwa Informacji;

10) wzór umowy powierzenia przetwarzania danych osobowych, stanowiącą załącznik nr 10 do niniejszej Polityki Bezpieczeństwa Informacji.

4. Przetwarzanie danych osobowych w Starostwie Powiatowym w Stargardzie jest dopuszczalne wyłącznie pod warunkiem przestrzegania ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych i wydanych na jej podstawie przepisów wykonawczych oraz niniejszej Polityki Bezpieczeństwa Informacji, a także instrukcji będących załącznikami do tej Polityki Bezpieczeństwa Informacji.

§ 2. Użyte w treści Polityki Bezpieczeństwa Informacji określenia oznaczają:

1) **ustawa** – ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;
2) **dane osobowe** – zestaw informacji pozwalających na jednoznaczną identyfikację konkretnej osoby w konkretnym środowisku pracy;
3) **zbiór danych osobowych** – dane osobowe zgromadzone w usystematyzowany sposób, pozwalający na łatwe dotarcie do konkretnej informacji;
4) **przetwarzanie danych** – wszystkie czynności wykonywane na danych, w tym szczególnie gromadzenie, utrwalanie, modyfikacja, usuwanie, przechowywanie, przenoszenie i przekazywanie, niezależnie od formy, w jakiej wykonywane są te czynności;
5) **anonimizacja** danych – takie przekształcenie danych osobowych, po którym nie można już przyporządkować poszczególnych informacji osobistych lub rzeczowych do określonej lub możliwej do zidentyfikowania osoby fizycznej albo można tego dokonać jedynie niewspółmiernie dużym nakładem czasu, kosztów i sił;
6) **Administrator Danych Osobowych** - Starosta Stargardzki, osoba funkcyjna odpowiedzialna za całokształt zagadnień związanych z przetwarzaniem danych osobowych w administrowanych przez nią zbiorach danych;
7) **Administrator Bezpieczeństwa Informacji** – osoba funkcyjna wyznaczana przez Administratora Danych Osobowych, odpowiedzialna za przestrzeganie zasad ochrony danych osobowych i nadzorująca bezpieczeństwo przetwarzania danych osobowych w Starostwie Powiatowym w Stargardzie;
8) **Administrator Systemu Informatycznego** – osoba funkcyjna wyznaczana przez Administratora Danych Osobowych odpowiedzialna za przestrzeganie zasad ochrony danych osobowych w systemie informatycznym i nadzorująca przetwarzanie danych osobowych w systemie informatycznym;
9) **system informatyczny** – zespół środków technicznych (urządzenia komputerowe, drukujące, łączności, wraz z okablowaniem i oprogramowaniem), zespół zabezpieczeń środków technicznych, użytkownicy tych urządzeń i programów, a także sieć informatyczna i udostępniane przez nią zasoby;
10) **osoby zatrudnione przy przetwarzaniu danych osobowych**, wszystkie osoby, w tym użytkownicy systemu informatycznego, mające, z racji wykonywanych obowiązków, dostęp do danych osobowych.

§ 3.1. Administrator Danych Osobowych ma obowiązek stosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczać dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Administrator Danych Osobowych określa zakres przetwarzanych danych osobowych w wydawanych zarządzeniach, regulaminach lub w indywidualnych umowach z podmiotami zewnętrznymi, którym zlecono przetwarzanie danych osobowych.

3. Administrator Danych Osobowych przetwarza dane osobowe znajdujące się w administrowanych przez niego zbiorach w określonych celach i w określonym zakresie, jeżeli:

1) jest to konieczne do realizacji określonych prawem zadań;
2) jest to niezbędne do osiągnięcia uzasadnionych celów;
3) w innym celu i zakresie, jeśli osoba, której przetwarzane dane dotyczą, wyrazi na to pisemną zgodę.

4. W przypadkach szczególnych cel i zakres przetwarzanych danych mogą określać i inne obowiązujące przepisy szczegółowe.

§ 4.1. Dostęp do zbioru danych osobowych oraz ich przetwarzania mają tylko osoby wpisane do ewidencji prowadzonej przez Administratora Bezpieczeństwa Informacji.

2. Osoby zatrudnione w Starostwie Powiatowym w Stargardzie przy przetwarzaniu danych osobowych są zobowiązane do przechowywania danych osobowych we właściwych zbiorach, nie dłużej niż jest to niezbędne dla osiągnięcia celu ich przetwarzania.

3. Osoby zatrudnione w Starostwie Powiatowym w Stargardzie przy przetwarzaniu danych osobowych przy wykorzystaniu systemów informatycznych są zobowiązane do postępowania zgodnie z „Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych", stanowiącą załącznik nr 4 Polityki Bezpieczeństwa Informacji.

§ 5. Osoby zatrudnione przy przetwarzaniu danych są zobowiązane powiadomić Administratora Bezpieczeństwa Informacji o ewentualnych naruszeniach bezpieczeństwa systemu ochrony danych osobowych w każdym zbiorze danych lub systemie. Tryb postępowania określa „Instrukcja postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych", stanowiąca załącznik nr 5 Polityki Bezpieczeństwa Informacji.

§ 6. W zbiorach danych administrowanych przez Starostwo Powiatowe w Stargardzie zabrania się przetwarzania danych ujawniających:

1) stan zdrowia;
2) pochodzenie rasowe lub etniczne;
3) poglądy polityczne;
4) przekonania religijne lub filozoficzne;
5) przynależność wyznaniową;
6) przynależność partyjną lub związkową;
7) kod genetyczny;
8) nałogi;
9) preferencje seksualne,

chyba że wymagają tego obowiązujące przepisy prawa lub osoba, której powyższe dane dotyczą, wyraziła pisemną zgodę.

§ 7. Pracownik, który:

1) przetwarza w zbiorze danych dane osobowe:
   a) do których przetwarzania nie jest upoważniony,
   b) których przetwarzanie jest zabronione,
   c) niezgodne z celem stworzenia zbioru danych;
2) udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym;
3) nie zgłasza Administratorowi Bezpieczeństwa Informacji zbiorów danych podlegających rejestracji;
4) nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o przysługujących jej prawach;
5) uniemożliwia osobie, której dane dotyczą, korzystanie z przysługujących jej praw,

podlega odpowiedzialności karnej zgodnie z ustawą oraz sankcjami określonymi w Kodeksie Pracy.

Rozdział 2
Gromadzenie danych osobowych

§ 8. Dane osobowe przetwarzane w Starostwie Powiatowym w Stargardzie mogą być uzyskiwane bezpośrednio od osób, których te dane dotyczą lub z innych źródeł, w granicach dozwolonych przepisami prawa.

§ 9.1. Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane.

2. W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.

Rozdział 3
Obowiązek informacyjny

§ 10.1. Kierownicy komórek organizacyjnych Starostwa Powiatowego w Stargardzie, w których są zbieranie i przetwarzane dane osobowe, są odpowiedzialni za poinformowanie osób, których dane osobowe przetwarzają, o:

1) adresie siedziby urzędu, pod którym dane są zbierane i przetwarzane;
2) celu zbierania danych, dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej;
3) prawie wglądu do treści swoich danych oraz możliwości ich poprawiania.

2. W przypadku zbierania danych osobowych nie bezpośrednio od osoby, której one dotyczą, osobę tę należy dodatkowo poinformować o źródle danych oraz o uprawnieniach wynikających z art. 32 ust. 1 pkt. 7 i 8 ustawy, tzn. wniesienia pisemnego żądania zaprzestania przetwarzania jej danych ze względu na szczególną sytuację oraz wniesienia sprzeciwu wobec przetwarzania jej danych, gdy Administrator Danych Osobowych zamierza je przetwarzać w celach marketingowych lub wobec przekazania jej danych osobowych innemu administratorowi.

§ 11.1. Materiały dotyczące innej niż ustawowa działalności Starostwa Powiatowego w Stargardzie mogą być wysyłane tylko do tych osób, które wcześniej wyraziły zgodę na piśmie na przetwarzanie ich danych osobowych w tym celu.

2. Kandydaci do pracy w Starostwie Powiatowym w Stargardzie, w procesie rekrutacji są zobowiązani podpisać pisemną zgodę na przetwarzanie ich danych osobowych.

3. Dokumenty złożone w celu określonym w ust. 2 są przechowywane w Biurze Obsługi Zarządu i Rady Powiatu i są włączane do akt osobowych pracownika.

4. Wzór formularza stosowanego dla spełnienia przez Starostwo Powiatowe w Stargardzie obowiązków wymienionych w ust. 1 i 2, stanowi załącznik 6 do niniejszej polityki bezpieczeństwa informacji.

Rozdział 4
Udzielanie informacji o przetwarzaniu danych osobowych

§ 12.1. Osobom, których dane osobowe przetwarza się w zbiorze danych Starostwa Powiatowego w Stargardzie, przysługuje, zgodnie z ustawą, prawo kontroli ich danych osobowych, a w szczególności prawo do uzyskania wyczerpujących informacji na temat tych danych.

2. Każda osoba, która wystąpi z wnioskiem o otrzymanie informacji, powinna otrzymać odpowiedź w formie pisemnej, w terminie nie dłuższym niż 30 dni od daty wpływu wniosku do Starostwa Powiatowego w Stargardzie.

3. Informacji, o której mowa w ust. 1, udziela się nie częściej niż raz na 6 miesięcy i powinna zawierać:

a) czy zbiór istnieje,
b) od kiedy dane są przetwarzane,
c) jakie jest źródło pozyskania danych,
d) w jaki sposób dane są udostępniane,
e) jaki jest cel i zakres przetwarzania danych,
f) w jakim zakresie i komu dane zostały udostępnione.

§ 13. W przypadku gdy dane osoby są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, Administrator Danych Osobowych jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

Rozdział 5
Rejestracja zbiorów danych osobowych

§ 14. Kierownicy komórek organizacyjnych Starostwa Powiatowego w Stargardzie, w których przetwarzane są dane osobowe, są zobowiązani do zgłoszenia Administratorowi Bezpieczeństwa Informacji na temat:

1) planowanego założenia nowych zbiorów danych osobowych wymagających rejestracji;
2) wnoszonych zmian do zbiorów już zarejestrowanych.

Rozdział 6
Ochrona przetwarzania danych osobowych

§ 15.1. Administrator Danych Osobowych Starostwa Powiatowego w Stargardzie wydaje imienne upoważnienia do przetwarzania danych osobowych. Administrator Bezpieczeństwa Informacji zobowiązany jest do ich ewidencjonowania i przechowywania. Upoważnienie może zostać wydane na czas określony lub do odwołania. Wzór formularza upoważnienia stanowi załącznik nr 7 do niniejszej Polityki Bezpieczeństwa Informacji.

2. Administrator Bezpieczeństwa Informacji Starostwa Powiatowego w Stargardzie zobowiązany jest także do zbierania, ewidencjonowania i przechowywania oświadczeń osób przetwarzających dane osobowe o zachowaniu w tajemnicy danych, z którymi mają styczność i środkach bezpieczeństwa stosowanych przy przetwarzaniu danych osobowych oraz oświadczeń osób zatrudnianych na podstawie umowy zlecenia, umowy o dzieło lub innej umowy cywilnej o zachowaniu tajemnicy. Wzory formularzy oświadczeń stanowi załącznik nr 8 do niniejszej Polityki Bezpieczeństwa Informacji.

3. Wyżej wymienione upoważnienia i oświadczenia przechowywany są także w aktach osobowych pracowników w Biurze Obsługi Zarządu i Rady Powiatu.

4. Brak ważnego upoważnienia, o którym mowa w pkt 1, oraz brak podpisanych oświadczeń o których mowa w pkt 2, ppkt 1 i 2, uniemożliwia powierzenie pracownikowi wykonywania zadań i obowiązków związanych z przetwarzaniem danych osobowych.

5. W celu ochrony przetwarzania i przechowywania danych osobowych stosuje się następujące środki techniczne:
1) budynek Starostwa Powiatowego przy ul. Skarbowej 1, jest zamykany po zakończeniu pracy i nadzorowany przez pracownika ochrony, w dni robocze od godz. 6.00 do godz. 22.00, a w godz. od 22.00 do godz. 6.00 i w dni wolne od pracy przez system alarmowy;
2) pomieszczenia urzędu w budynku przy ul. Bogusława IV 21, zabezpieczone są zamkami patentowymi, a wejście do budynku zabezpieczono kodem;
3) pomieszczenia urzędu w budynku przy ul. Rynek Staromiejski 5, zabezpieczone są zamkami patentowymi. Budynek monitorowany jest, w dni powszednie od godz. 15.30 do godz. 7.30, a w dni świąteczne i wolne od pracy całodobowo, przez system alarmowy;
4) pomieszczenia urzędu w budynku przy ul. Staszica zabezpieczone są kratami w oknach i dwoma zamkami patentowymi, a także całodobową ochroną przez firmę ochroniarską;
5) pomieszczenia w których przetwarzane są dane w budynku starostwa zabezpieczone są zamkami patentowymi. Instrukcję zarządzania kluczami w Starostwie Powiatowym w Stargardzie stanowi załącznik nr 9 do niniejszej Polityki Bezpieczeństwa Informacji.

§ 16.1. Całkowity nadzór i kontrolę przetwarzania danych osobowych w Starostwie Powiatowym w Stargardzie realizuje i odpowiada za te działania Administrator Bezpieczeństwa Informacji.

2. Administrator Bezpieczeństwa Informacji ma obowiązek ściśle współpracować z Administratorem Systemu Informatycznego w zakresie przetwarzania danych osobowych w systemach informatycznych.

3. Administrator Bezpieczeństwa Informacji ma obowiązek zapewnić zapoznanie się osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami dotyczącymi ochrony danych osobowych oraz przeszkolić je w tym zakresie.

§ 17.1. W celu realizacji powierzonych zadań Administrator Bezpieczeństwa Informacji w Starostwie Powiatowym w Stargardzie ma prawo:

1) kontrolować komórki organizacyjne Starostwa Powiatowego w Stargardzie, w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarzane są dane osobowe;
2) wydawać polecenia kierownikom komórek organizacyjnych Starostwa Powiatowego w Stargardzie, w zakresie bezpieczeństwa danych osobowych;
3) informować Administratora Danych Osobowych Starostwa Powiatowego w Stargardzie o przypadkach naruszenia bezpieczeństwa danych osobowych;
4) żądać od wszystkich pracowników Starostwa Powiatowego w Stargardzie wyjaśnień w sytuacjach naruszenia bezpieczeństwa danych osobowych.

Rozdział 7
Zasady udostępniania danych osobowych

§ 18. Administrator Danych Osobowych udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

§ 19.1. Zbiory danych osobowych udostępnia się na pisemny, umotywowany wniosek, chyba że odrębne przepisy prawa stanowią inaczej.

2. Wniosek o udostępnienie danych osobowych powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie.

3. Wniosek o udostępnienie danych osobowych jest rozpatrywany przez Administratora Bezpieczeństwa Informacji, który jednocześnie prowadzi ewidencję wniosków.

4. Decyzję w sprawie udostępnienia danych podejmuje Administrator Bezpieczeństwa Informacji.

§ 20. Administrator Danych Osobowych może odmówić udostępnienia danych osobowych, jeżeli spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą, lub innych osób oraz jeżeli dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.

§ 21.1. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej. Wzór formularza umowy stanowi załącznik nr 10 do niniejszej Polityki Bezpieczeństwa Informacji.

2. Podmiot, o którym mowa w ust. 1, jest zobowiązany do zastosowania środków organizacyjnych i technicznych, zabezpieczających zbiór przed dostępem osób nieupoważnionych na zasadach określonych w przepisach o ochronie danych osobowych.

3. Podmiot, o którym mowa w ust. 1, jest zobowiązany przetwarzać dane osobowe wyłącznie w zakresie określonym w umowie.

4. W przypadkach opisanych w ust. 1–3 odpowiedzialność za ochronę przetwarzanych danych osobowych spoczywa na Administratorze Danych Osobowych, co nie wyłącza z odpowiedzialności podmiotu, z którym zawarto umowę z tytułu przetwarzania danych niezgodnie z ustawą.

STAROSTA

Załącznik nr 1
do Polityki
Bezpieczeństwa Informacji

Wykaz budynków i pomieszczeń, w których przetwarzane są dane osobowe

Obszary przetwarzania danych w pomieszczeniach budynku przy ul. Skarbowej 1
poziom -1

Lp.	Nr pokoju	Komórka organizacyjna
1.	002, 003, 005	Biuro Obsługi Urzędu
2.	006	Wydział Komunikacji

Parter

Lp.	Nr pokoju	Komórka organizacyjna
4.	04, 05, 06,	Biuro Zamówień
5.	07, 08, 09, 10, 11, 12	Wydział Komunikacji
6.	Kancelaria ogólna, 02, 03	Biuro Obsługi Urzędu

I piętro – lewe skrzydło

Lp.	Nr pokoju	Komórka organizacyjna
7.	104, 106, 107, 108, 114 (sekretariat)	Biuro Obsługi Zarządu i Rady Powiatu

I piętro – prawe skrzydło

Lp.	Nr pokoju	Komórka organizacyjna
8.	118	Wydział Zarządzania Bezpieczeństwem
9.	119, 120	Powiatowy Zespół ds. Orzekania o Niepełnosprawności
10.	117, 117A	Wydział Środowiska

II piętro – lewe skrzydło

Lp.	Nr pokoju	Komórka organizacyjna
11.	204,205, 206, 207, 208, 209, 210	Wydział Gospodarki Nieruchomościami
12.	211, 212, 215, 216	Wydział Oświaty, Kultury i Sportu
13.	213, 214	Wydział Planowania i Rozwoju

II piętro – prawe skrzydło

Lp.	Nr pokoju	Komórka organizacyjna
14.	218, 222, 223, 224	Wydział Urbanistyki, Architektury i Budownictwa
15.	219	Wydział Oświaty, Kultury i Sportu
16.	220	Powiatowy Rzecznik Konsumentów

III piętro – prawe skrzydło

Lp.	Nr pokoju	Komórka organizacyjna
17.	301, 302, 303, 304, 305, 306, 307, 308	Wydział Finansowy

Obszary przetwarzania danych w pomieszczeniach przy ul. Rynek Staromiejski 5

Lp.	Nr pokoju	Komórka organizacyjna
18.	106,107,109,110,11,112,113,125, 126, 128,130,	Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej

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

Lp.	Nr pokoju	Komórka organizacyjna
19.	215,218	Wydział Zarządzania Bezpieczeństwem
20.	216, 217	Wydział Audytu i Kontroli

Obszary przetwarzania danych w pomieszczeniach budynku przy ul. Staszica 27

Lp.	Nr pokoju	Komórka organizacyjna
21.	Archiwum pomocnicze	Powiatowy Zespół ds. Orzekania o Niepełnosprawności

STAROSTA
Iwona Wiśniewska

Załącznik nr 2
Do Polityki
Bezpieczeństwa Informacji

Wykaz zbiorów danych osobowych oraz programy zastosowane do przetwarzania tych danych

Lp.	Zbiór danych osobowych	Program zastosowany do przetwarzania danych osobowych/sposób przetwarzania
1.	Zbiór osób pobierających świadczenie pieniężne	Program Kadry -Płace
2.	Zbiór osób zgłaszanych do ubezpieczenia społecznego	Program Płatnik
3.	Zbiór osób posiadających prawo użytkowania wieczystego /opłaty Skarbu Państwa	Program Powiat Informix
4.	Zbiór (ewidencja) właścicieli pojazdów	Program POJAZD
5.	Zbiór (ewidencja) kierowców	Program KIEROWCA
6.	Zbiór osób będących właścicielami gruntów i budynków/Ewidencja gruntów i budynków	Program GEOINFO7
7.	Zbiór/Rejestr strażników społecznej straży rybackiej	Dane przetwarzane w sposób tradycyjny
8.	Zbiór/Rejestr sprzętu pływającego do sportowego połowu ryb	Baza danych w formie pliku tekstowego
9.	Zbiór/Rejestr wydanych kart wędkarskich	Baza danych w formie pliku tekstowego
10.	Zbiór/Rejestr posiadaczy żywych zwierząt gatunków wymienionych w załącznikach A i B rozporządzenia Rady (WE) 333/97 z dnia 9 grudnia 1996 r.	Dane przetwarzane w sposób tradycyjny
11.	Zbiór/Rejestr zezwoleń na wykonywanie zawodu przewoźnika drogowego osób i rzeczy	Dane przetwarzane w sposób tradycyjny
12.	Zbiór/Rejestr instruktorów nauki jazdy	Dane przetwarzane w sposób tradycyjny
13.	Zbiór/Rejestr imiennych uprawnień do wykonywania badań technicznych pojazdów	Dane przetwarzane w sposób tradycyjny
14.	Zbiór/Rejestr przedsiębiorców prowadzących ośrodki szkolenia kierowców	Dane przetwarzane w sposób tradycyjny
15.	Zbiór/Rejestr wniosków o wydanie zezwolenia na sprowadzenie zwłok	Dane przetwarzane w sposób tradycyjny
16.	Zbiór/Rejestr rzeczy znalezionych	Dane przetwarzane w sposób tradycyjny

17.	Zbiór/Rejestr wniosków konsumentów o udzielenie pomocy prawnej przez Powiatowego Rzecznika Konsumentów	Dane przetwarzane w sposób tradycyjny
18.	Zbiór danych osób ubiegających się o awans zawodowy nauczycieli	Dane przetwarzane w sposób tradycyjny
19.	Zbiór/Rejestr osób prowadzących szkoły i placówki niepublicznych prowadzonych na terenie Powiatu Stargardzkiego	Dane przetwarzane w sposób tradycyjny
20.	Zbiór/Rejestr osób odbywających karę prac społecznie użytecznych	Dane przetwarzane w sposób tradycyjny
21.	Zbiór/Rejestr użytkowników wieczystych Skarbu Państwa	Dane przetwarzane w sposób tradycyjny
22.	Zbiór/Rejestr właścicieli lasów nie stanowiących własności Skarbu Państwa	Dane przetwarzane w systemie Geo-Info oraz w sposób tradycyjny
23.	Zbiór/ Rejestr osób składających skargi i wnioski	Dane przetwarzane w sposób tradycyjny
24.	Zbiór danych osób stawiających się do kwalifikacji wojskowej	Dane przetwarzane w sposób tradycyjny
25.	Zbiór/Rejestr osób występujących o pozwolenie na budowę	Dane przetwarzane w sposób tradycyjny
26.	Zbiór/Rejestr osób ubiegających się o zaświadczenie o samodzielności lokali	Dane przetwarzane w sposób tradycyjny
27.	Zbiór/Rejestr osób którym zwrócono nieruchomości	Dane przetwarzane w sposób tradycyjny
28.	Zbiór/Wykaz Radnych Rady Powiatu	Dane przetwarzane w sposób tradycyjny
29.	Zbiór (rejestr) wydanych legitymacji osoby niepełnosprawnej	Program EKSMOON
30.	Zbiór (rejestr) wniosków o wydanie orzeczenia o niepełno-sprawności	Program EKSMOON
31.	Zbiór wydanych kart parkingowych	Program EKSMOON
32.	Zbiór (rejestr) nieletnich kierowanych do ośrodków socjoterapii, ośrodków szkolno wychowawczych, ośrodków wychowawczych, i szkoły specjalnej w Stargardzie	Dane przetwarzane w sposób tradycyjny
33.	Zbiór (rejestr) przedsiębiorców prowadzących stacje kontroli pojazdów	Dane przetwarzane w sposób tradycyjny
34.	Zbiór (rejestr) klubów sportowych	Dane przetwarzane w sposób tradycyjny
35.	Zbiór (rejestr) sprzętu pływającego do zawodowego połowu ryb	Dane przetwarzane w sposób tradycyjny

STAROSTA

Iwona Wiśniewska

Załącznik nr 3
Do Polityki
Bezpieczeństwa Informacji

Opis struktury zbiorów danych osobowych przetwarzanych w systemach informatycznych oraz sposób przepływu danych pomiędzy systemami informatycznymi

Lp	Nazwa	Systemy informatyczne	Cel przetwarzania	Kategoria osób	Zakres przetwarzanych danych	Uwagi
1.	Zbiór osób pobierających świadczenie pieniężne w Starostwie	Kadry -Płace	Naliczenie płac.	Osoby fizyczne (pracownicy Starostwa)	Dane osobowe osób fizycznych(pracowników Starostwa) odbierających świadczenie pieniężne na podstawie stosunków prawnych łączących ich ze Starostwem. Zakres informacji: 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(imię nazwisko, data urodzenia).	
2.	Zbiór osób zgłaszanych do ubezpieczenia społecznego	Płatnik	Zgłaszanie pracowników Starostwa do ubezpieczenia społecznego.	Osoby fizyczne (pracownicy Starostwa).	Dane osób fizycznych zgłaszanych do ubezpieczenia społecznego. Zakres informacji: nazwiska, imiona, imiona rodziców, data i miejsce urodzenia, miejsce zamieszkania (województwo, powiat, gmina, miejscowość, ulica, nr domu), NIP, PESEL.	
3.	Zbiór osób płacących opłaty Skarbu Państwa	Powiat Informix	Naliczanie opłat od osób fizycznych	Osoby fizyczne posiadające prawo użytkowania wieczystego nieruchomości skarbu państwa	Dane osób fizycznych posiadających prawo użytkowania wieczystego nieruchomości skarbu państwa. Zakres informacji prowadzonych w zbiorze; imię, nazwisko i adres zamieszkania.	

Lp	Nazwa	Systemy informatyczne	Cel przetwarzania	Kategoria osób	Zakres przetwarzanych danych	Uwagi
4.	Zbiór (ewidencja) właścicieli pojazdów.	POJAZD	Ewidencja właścicieli pojazdów	Osoby fizyczne będące właścicielami pojazdów	Dane osób fizycznych będących właścicielami pojazdów zakres informacji prowadzonych w zbiorze: imiona, nazwisko, data i miejsce urodzenia, adres zamieszkania, nr PESEL, nr i seria dowodu osobistego, imiona rodziców, nr dowodu rejestracyjnego, nr tablic rejestracyjnych.	Administratorem Danych jest Ministerstwo Spraw Wewnętrznych i Administracji
5.	Zbiór (ewidencja) kierowców	KIEROWCA	Ewidencja kierowców	Osoby fizyczne będące kierowcami	Dane osób fizycznych będących kierowcami. Zakres informacji prowadzonych w zbiorze: imiona, nazwisko, data i miejsce urodzenia, adres zamieszkania, nr PESEL, nr i seria dowodu osobistego, imiona rodziców, nr i seria dowodu osobistego, informacje dotyczące prawa jazdy, informacje dotyczące stanu zdrowia.	Administratorem Danych jest Ministerstwo Spraw Wewnętrznych i Administracji
6.	Zbiór (rejestr) przedsię-biorców prowadzących ośrodki szkolenia kierowców	Zbiór prowadzony poza systemem informa-tycznym	Ewidencja ośrodków szkolenia kierowców	Osoby fizyczne prowadzące ośrodki szkolenia kierowców	Dane osób fizycznych prowadzących ośrodki szkolenia kierowców. Zakres informacji prowadzonych w zbiorze: imiona, nazwisko, imiona rodziców, data i miejsce urodzenia, adres zamieszkania, nr PESEL, NIP, wykształcenie, nr i seria dowodu osobistego, dane indentyfikacyjne przedsiębiorcy oraz pojazdów będących własnością przedsiębiorcy.	Dane pozyskiwane od osób, których dotyczą

Lp	Nazwa	Systemy informatyczne	Cel przetwarzania	Kategoria osób	Zakres przetwarzanych danych	Uwagi
7.	Zbiór (rejestr) stacji kontroli pojazdów	Zbiór prowadzony w systemie informa-tycznym i poza systemem informa-tycznym	Ewidencja stacji kontroli pojazdów	Osoby fizyczne prowadzące stacje kontroli pojazdów	Dane osób fizycznych prowadzących stacje kontroli pojazdów. Zakres informacji prowadzonych w zbiorze: imiona, nazwisko, imiona rodziców, data i miejsce urodzenia, adres zamieszkania, nr PESEL, NIP, wykształcenie, nr i seria dowodu osobistego, dane indentyfikacyjne przedsiębiorcy.	Dane pozyskiwane od osób, których dotyczą
8.	Zbiór (rejestr) instruktorów nauki jazdy	Zbiór prowadzony w systemie informa-tycznym. i poza systemem informa-tycznym	Ewidencja instruktorów nauki jazdy	Osoby fizyczne ubiegające się o wydanie legitymacji instruktora nauki jazdy	Dane osób fizycznych ubiegających się o wydanie legitymacji instruktora nauki jazdy. Zakres informacji prowadzonych w zbiorze: imiona, nazwisko, imiona rodziców, data i miejsce urodzenia, adres zamieszkania, nr PESEL, NIP, wykształcenie, nr i seria dowodu osobistego, stan zdrowia, dane o karalności.	Dane pozyskiwane od osób, których dotyczą
9.	Zbiór (rejestr) zezwoleń na dokonywanie zawodu przewoźnika drogowego osób lub rzeczy	Zbiór prowadzony w systemie informa-tycznym i poza systemem informa-tycznym	Ewidencja osób posiadających zezwolenia na dokonywanie zawodu przewoźnika drogowego osób lub rzeczy	Osoby posiadające zezwolenia na dokonywani e zawodu przewoźnika drogowego osób lub rzeczy	Dane osób fizycznych prowadzących działalność w zakresie transportu osób i rzeczy. Zakres informacji prowadzonych w zbiorze: imiona, nazwisko, imiona rodziców, data i miejsce urodzenia, adres zamieszkania, nr PESEL, NIP, seria i nr dowodu osobistego, dane o karalności a także informacje dotyczące prowadzonej działalności, dane pojazdów znajdujących się w posiadaniu przedsiębiorcy.	Dane pozyskiwane od osób, których dotyczą

Lp	Nazwa	Systemy informatyczne	Cel przetwarzania	Kategoria osób	Zakres przetwarzanych danych	Uwagi
10.	Ewidencja gruntów i budynków powiatu stargardzkiego	GEOINFO7	Ewidencja właścicieli gruntów i budynków	Dane osób będących właścicielami gruntów i budynków	Osoby fizyczne będące właścicielami gruntów i budynków. Zakres informacji prowadzonych w zbiorze: imiona, nazwisko, adres zamieszkania, PESEL.	Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej
11.	Zbiór (rejestr) strażników społecznej straży rybackiej powiatu stargardzkiego.	Zbiór prowadzony w systemie informa-tycznym i poza systemem informa-tycznym	Ewidencja strażników społecznej straży rybackiej	Osoby fizyczne będące strażnikami społecznej straży rybackiej	Dane osób ubiegających się o wydanie legitymacji strażnika społecznej straży rybackiej powiatu stargardzkiego. Zakres informacji prowadzonych w zbiorze: imiona, nazwisko, data urodzenia adres zamieszkania.	Dane pozyskiwane od osób, których dotyczą

Lp	Nazwa	Systemy informatyczne	Cel przetwarzania	Kategoria osób	Zakres przetwarzanych danych	Uwagi
12.	Zbiór (rejestr) sprzętu pływającego służącego do amatorskiego połowu ryb.	Zbiór prowadzony w systemie informa-tycznym i poza systemem informa-tycznym	Ewidencja posiadaczy sprzętu pływającego służącego do amatorskiego połowu ryb	Osoby fizyczne będące posiadaczami sprzętu pływającego służącego do amatorskiego połowu ryb	Dane osób fizycznych składających wniosek o rejestrację sprzętu pływającego służącego do amatorskiego połowu ryb. Zakres informacji prowadzonych w zbiorze: imiona, nazwisko, adres zamieszkania.	Dane pozyskiwane od osób, których dotyczą
13.	Zbiór (rejestr) wydanych kart wędkarskich	Zbiór prowadzony w systemie informa-tycznym i poza systemem informa-tycznym	Ewidencja osób fizycznych posiadających kartę wędkarską	Osoby fizyczne posiadające uprawnienia (kartę wędkarską) do amatorskiego połowu ryb	Dane osób fizycznych, którym wydano kartę wędkarską. Zakres informacji prowadzonych w zbiorze: imiona, nazwisko, data i miejsce urodzenia, adres zamieszkania.	Dane pozyskiwane od osób, których dotyczą
14.	Zbiór(rejestr) posiadaczy żywych zwierząt gatunków wymienionych załącznikach A i B rozporz. Rady (WE) nr 338/97 z dnia 9 grudnia 1996r.	Zbiór prowadzony w systemie informa-tycznym i poza systemem informa-tycznym	Ewidencja zwierząt chronionych	Osoby fizyczne posiadające zwierzęta chronione oraz osoby będące źródłami pochodzenia zwierzęcia chronionego	Dane osób posiadających zwierzęta chronione oraz osób będących źródłami pochodzenia zwierzęcia chronionego . Zakres informacji prowadzonych w zbiorze: imiona, nazwisko, adres zamieszkania oraz w przypadku osób posiadających zwierzęta chronione, adres miejsca przetrzymywania zwierzęcia.	Dane pozyskiwane od osób, których dotyczą

Lp	Nazwa	Systemy informatyczne	Cel przetwarzania	Kategoria osób	Zakres przetwarzanych danych	Uwagi
15.	Zbiór (rejestr) wniosków o wydanie zezwolenia na sprowadzenie zwłok z zagranicy	Zbiór prowadzony w systemie informa-tycznym i poza systemem informa-tycznym	Ewidencja wniosków i decyzji w sprawie zezwolenia na sprowadzenie zwłok z zagranicy	Dane osobowe osób składających wnioski o wydanie zezwolenia na sprowadzenie zwłok z zagranicy	Dane osób ubiegających się o zezwolenia na sprowadzenie zwłok z zagranicy . Zakres informacji prowadzonych w zbiorze: imiona, nazwisko, adres zamieszkania, nr telefonu.	Dane pozyskiwane od osób, których dotyczą
16.	Zbiór (rejestr) rzeczy znalezionych	Zbiór prowadzony w systemie informa-tycznym i poza systemem informa-tycznym	Ewidencja rzeczy znalezionych	Dane osobowe osób zawiadamiający ch o znalezieniu rzeczy oraz osób upoważnionych do jej odbioru	Dane osób ubiegających się o zezwolenia na sprowadzenie zwłok z zagranicy . Zakres informacji prowadzonych w zbiorze: imiona, nazwisko, adres zamieszkania, nr telefonu.	Dane pozyskiwane od osób, których dotyczą
17.	Zbiór (rejestr) wniosków konsumentów o udzielenie pomocy prawnej przez Powiatowego Rzecznika Konsumentów	Zbiór prowadzony w systemie informa-tycznym i poza systemem informa-tycznym	Ewidencja wniosków konsumentów o udzielenie pomocy prawnej przez Powiatowego Rzecznika Konsumentów	Dane osobowe konsumentów	Dane osób ubiegających się o udzielenie pomocy prawnej przez Powiatowego Rzecznika Konsumentów. Zakres informacji prowadzonych w zbiorze: imiona, nazwisko, adres zamieszkania, nr telefonu.	Dane pozyskiwane od osób, których dotyczą

Lp	Nazwa	Systemy informatyczne	Cel przetwarzania	Kategoria osób	Zakres przetwarzanych danych	Uwagi
18.	Zbiór (rejestr) awansu zawodowego nauczycieli	Zbiór prowadzony w systemie informa-tycznym i poza systemem informa-tycznym	Ewidencja nauczycieli ubiegających się o awans zawodowy	Dane osób (nauczycieli) ubiegających się o awans zawodowy	Dane osobowe nauczycieli ubiegających się o awans zawodowy. Zakres informacji prowadzonych w zbiorze: imiona, nazwisko, data i miejsce urodzenia adres zamieszkania, miejsce pracy, zawód, wykształcenie, seria i nr dowodu osobistego.	Dane pozyskiwane od osób, których dotyczą
19.	Zbiór (rejestr) szkół i placówek niepublicznych prowadzonych na terenie powiatu stargardzkiego	Zbiór prowadzony w systemie informa-tycznym i poza systemem informa-tycznym	Ewidencja szkół i placówek niepublicznych powiatu stargardzkiego	Dane osób fizycznych prowadzących szkołę i placówkę niepubliczną oraz nauczycieli i pracowników tych szkół i placówek.	Dane osobowe osób prowadzących szkołę i placówkę niepubliczną oraz nauczycieli i pracowników tych szkół i placówek. Zakres informacji prowadzonych w zbiorze: imiona, nazwiska, daty i miejsca urodzeń, adres zamieszkania, nr PESEL, miejsce pracy, zawód, wykształcenie, seria i nr dowodu osobistego, nr telefonu.	Dane pozyskiwane od osób, których dotyczą
20.	Zbiór (rejestr) osób skazanych odbywających karę prac społeczno-użytecznych	Zbiór prowadzony w systemie informa-tycznym i poza systemem informa-tycznym	Ewidencja osób skazanych na karę prac społeczno-użytecznych	Dane osób skazanych na karę prac społeczno-użytecznych	Dane osobowe osób skazanych na kare prac społeczno-użytecznych . Zakres informacji prowadzonych w zbiorze: imiona, nazwiska, imiona rodziców, data i miejsce urodzenia, adres zamieszkania, wymiar kary ograniczenia wolności.	Dane pozyskiwane ze źródeł zewnętrznych

Lp	Nazwa	Systemy informatyczne	Cel przetwarzania	Kategoria osób	Zakres przetwarzanych danych	Uwagi
21.	Zbiór (rejestr) użytkowników wieczystych Skarbu Państwa	Zbiór prowadzony w systemie informa-tycznym	Ewidencja osób fizycznych posiadających prawo do użytkowania wieczystego	Dane osób fizycznych posiadających prawo do użytkowania wieczystego	Dane osób fizycznych posiadających prawo do użytkowania wieczystego. Zakres informacji prowadzonych w zbiorze: imiona, nazwiska, imiona rodziców, adres zamieszkania lub pobytu, nr PESEL, NIP, seria i nr dowodu osobistego.	
22.	Zbiór (rejestr) właścicieli lasów nie stanowiących własności Skarbu Państwa	Zbiór prowadzony w systemie informa-tycznym i poza systemem informa-tyczny	Ewidencja lasów nie stanowiących własności Skarbu Państwa	Dane osób właścicieli lasów nie stanowiących własności Skarbu Państwa	Dane osób fizycznych posiadających prawo własności lasów nie stanowiących własności Skarbu Państwa. Zakres informacji prowadzonych w zbiorze: imiona, nazwiska, adres zamieszkania, nr telefonu.	
23.	Zbiór (rejestr) skarg i wniosków	Zbiór prowadzony poza systemem informa-tyczn	Ewidencja skarg i wniosków	Dane osób składających wnioski i skargi	Dane osób fizycznych składających wnioski i skargi. Zakres informacji prowadzonych w zbiorze: imiona, nazwiska, adres zamieszkania, nr telefonu.	Dane pozyskiwane od osób, których dotyczą

Lp	Nazwa	Systemy informatyczne	Cel przetwarzania	Kategoria osób	Zakres przetwarzanych danych	Uwagi
24.	Zbiór osób stawiających się do kwalifikacji w danym roku	Zbiór prowadzony poza systemem informa-tycznym	Ewidencja osób stawiających się do kwalifikacji wojskowej w danym roku	Dane osób stawiających się do kwalifikacji wojskowej w danym roku	Dane osób fizycznych stawiających się do kwalifikacji wojskowej w danym roku. Zakres informacji prowadzonych w zbiorze: imiona, nazwiska, imiona rodziców, data i miejsce urodzenia adres zamieszkania, nr książeczki wojskowej, kategoria zdolności do służby wojskowej, stan zdrowia.	
25.	Zbiór (rejestr) pozwoleń na budowę	Zbiór prowadzony w systemie informa-tycznym i poza systemem informa-tycznym	Ewidencja osób starających się o pozwolenie na budowę	Dane osób starających się o pozwolenie na budowę	Dane osób starających się o pozwolenie na budowę . Zakres informacji prowadzonych w zbiorze: imiona, nazwiska, adres zamieszkania.	Dane pozyskiwane od osób, których dotyczą
26.	Zbiór (rejestr) zaświadczeń o samodzielności lokali	Zbiór prowadzony w systemie informatyczn ym i poza systemem informa-tycznym	Ewidencja osób składających wnioski o samodzielność lokali (mieszkalnych, użytkowych)	Dane osób składających wnioski o samodzielność lokali (mieszkalnych, użytkowych)	Dane osób składających wnioski o samodzielność lokali (mieszkalnych, użytkowych). Zakres informacji w zbiorze: imiona, nazwisko, adres.	Dane pozyskiwane od osób, których dotyczą

Lp	Nazwa	Systemy informatyczne	Cel przetwarzania	Kategoria osób	Zakres przetwarzanych danych	Uwagi
27.	Zbiór (rejestr) osób, którym przysługuje zwrot nieruchomości	Zbiór prowadzony w systemie informa-tycznym i poza systemem informa-tycznym	Ewidencja osób, którym przysługuje zwrot nieruchomości	Dane osób, którym przysługuje zwrot nieruchomości	Dane osób, którym przysługuje zwrot nieruchomości. Zakres informacji prowadzonych w zbiorze: imiona, nazwisko, imiona rodziców, adres zamieszkania	
28.	Zbiór (rejestr) wniosków o wydanie orzeczenia o niepełno-sprawności	Program EKSMOON	Ewidencja wniosków o wydanie orzeczenia o niepełno-sprawności	Dane osób, ubiegających się o wydanie orzeczenia o niepełno-sprawności	Dane osób, ubiegających się o wydanie orzeczenia o niepełnosprawności. Zakres informacji prowadzonych w zbiorze: imię, nazwisko, data i miejsce urodzenia, nr i seria dowodu osobistego, PESEL, adres zamieszkania.	Ministerstwo Rodziny i Polityki Społecznej (Biuro Pełnomocnika Rządu ds. Osób Niepełnospra-wnych)
29.	Zbiór wydanych kart parkingowych	Program EKSMOON	Ewidencja osób, którym wydano kartę parkingową	Dane osób, którym wydano kartę parkingową	Dane osób, którym wydano kartę parkingową. Zakres informacji prowadzonych w zbiorze: imię, nazwisko, adres zamieszkania, PESEL.	Ministerstwo Rodziny i Polityki Społecznej (Biuro Pełnomocnika Rządu ds. Osób Niepełnospra-wnych)

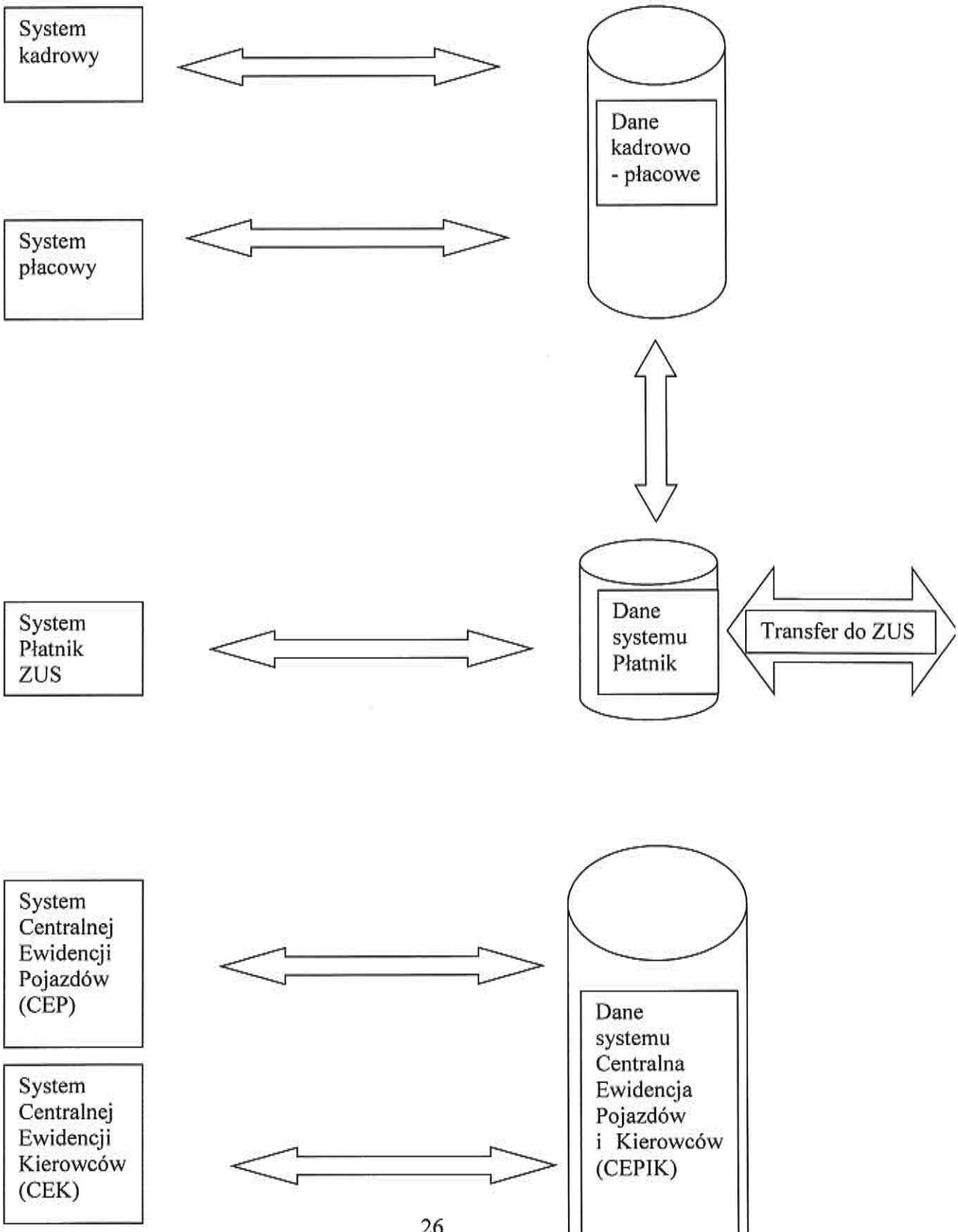
Lp	Nazwa	Systemy informatyczne	Cel przetwarzania	Kategoria osób	Zakres przetwarzanych danych	Uwagi
30.	Zbiór (rejestr) wydanych legitymacji osoby niepełno-sprawnej	Program EKSMOON	Ewidencja wydanych legitymacji osoby niepełno-sprawnej	Dane osób, którym wydano legitymację osoby niepełno-sprawnej	Dane osób, którym wydano legitymację osoby niepełnosprawnej. Zakres informacji prowadzonych w zbiorze; imię, nazwisko, data i miejsce urodzenia, nr i seria dowodu osobistego, PESEL, adres zamieszkania stopień niepełnosprawności.	Ministerstwo Rodziny i Polityki Społecznej (Biuro Pełnomocnika Rządu ds. Osób Niepełnospra-wnych)
31.	Zbiór (wykaz) Radnych Powiatu Stargardzkiego	Zbiór prowadzony w systemie informa-tycznym i poza systemem informa-tycznym	Ewidencja Radnych powiatu Stargardzkiego	Dane osób będących Radnymi Powiatu Stargardzkiego	Dane osób będących Radnymi Powiatu Stargardzkiego. Zakres informacji prowadzonych w zbiorze: imiona, nazwiska, adres zamieszkania, data i miejsce urodzenia, nr PESEL, NIP, miejsce pracy, zawód, wykształcenie, seria i nr dowodu osobistego.	Dane pozyskiwane od osób, których dotyczą
32.	Zbiór (rejestr) nieletnich kierowanych do ośr. Socjoterapii, ośr. szkolno-wychowa-wczych i szkoły specjalnej	Zbiór prowadzony w systemie informa-tycznym i poza systemem informa-tycznym	Wydanie skierowania dla nieletnich kierowanych do ośr. socjoterapii, ośr. szkolno-wychowa-wczych	Dane osób nieletnich kierowanych do ośr. socjoterapii, ośr. szkolno-wychowa-wczych i szkoły specjalnej	Dane osób nieletnich kierowanych do ośr. socjoterapii, ośr. szkolno-wychowawczych, ośr. wychowawczych i szkoły specjalnej w Stargardzie. Zakres informacji prowadzonych w zbiorze: imiona, nazwiska, adres zamieszkania, data i miejsce urodzenia, nr PESEL, orzeczenie o potrzebie kształcenia specjalnego, karta zdrowia, karta szczepień.	Dane pozyskiwane ze źródeł zewnętrznych

Lp	Nazwa	Systemy informatyczne	Cel przetwarzania	Kategoria osób	Zakres przetwarzanych danych	Uwagi
33	Zbiór (rejestr) przedsiębiorców prowadzących stacje kontroli pojazdów	Zbiór prowadzony w systemie informatycznym i poza systemem informatycznym	Ewidencja przedsiębiorców prowadzących stacje kontroli pojazdów	Dane osób prowadzących stacje kontroli pojazdów	Dane osób prowadzących stacje kontroli pojazdów. Zakres informacji prowadzonych w zbiorze: imiona, nazwiska, adres firmy, kod stacji, adres stacji kontroli pojazdów, nr KRS, nr NIP.	Dane pozyskiwane od osób, których dotyczą
34.	Zbiór (rejestr) klubów sportowych	Zbiór prowadzony w systemie informatycznym i poza systemem informatycznym	Ewidencja założycieli i członków klubów sportowych	Dane osób założycieli i członków klubów sportowych	Dane osób założycieli i członków klubów sportowych. Zakres informacji prowadzonych w zbiorze: imiona, nazwiska, nr PESEL, adres zamieszkania.	Dane pozyskiwane od osób, których dotyczą
35.	Zbiór (rejestr) do zawodowego połowu ryb	Zbiór prowadzony w systemie informatycznym i poza systemem informatycznym	Ewidencja posiadaczy sprzętu pływającego służącego do zawodowego połowu ryb	Osoby fizyczne będące posiadaczami sprzętu pływającego służącego do zawodowego połowu ryb	Dane osób fizycznych składających wniosek o rejestrację sprzętu pływającego służącego do zawodowego połowu ryb. Zakres informacji prowadzonych w zbiorze: imiona, nazwisko, adres zamieszkania.	Dane pozyskiwane od osób, których dotyczą

STAROSTA

Iwona Wiśniewska

PRZEPŁYW DANYCH OSOBOWYCH



STAROSTA
Iwona Wiśniewska

Załącznik nr 4
do Polityki
Bezpieczeństwa Informacji

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Rozdział 1
Postanowienia ogólne, definicje i objaśnienia

§1.1 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 Stargardzie.

2. Ilekroć w instrukcji jest mowa o:

1) **rozporządzeniu** – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024);
2) **zasadzie czystego biurka** – rozumie się nie pozostawianie na biurku, dokumentów papierowych i ruchomych nośników danych (płyty CD, DVD, BD, dyski przenośne, pamięci zewnętrzne) zawierających dane osobowe, po pracy i w czasie przerw w pracy wymagających odejścia od biurka. W momencie, gdy nie są używane, powinny być zabezpieczone w zamykanych na klucz szufladach lub szafach;
3) **osobie upoważnionej do przetwarzania danych osobowych** – rozumie się przez to osobę zatrudnioną na podstawie umowy o pracę, umowy zlecenia lub innej umowy, osobę odbywającą u administratora danych staż absolwencki, praktykę studencką, wolontariat, której nadane zostało przez administratora danych upoważnienie do przetwarzania danych osobowych;
4) **użytkowniku** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano uprawnienia do przetwarzania danych w systemie informatycznym;
5) **sieci lokalnej** – należy przez to rozumieć połączenie systemów informatycznych Starostwa Powiatowego w Stargardzie wyłącznie do własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych;
6) **sieci rozległej** – należy przez to rozumieć sieć publiczną łączącą sieci lokalne, inne (mniejsze) sieci rozległe oraz pojedyncze komputery. Najpopularniejszym przykładem sieci rozległych jest Internet;

7) **systemie informatycznym administratora danych** – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych;
8) **identyfikatorze użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w wyznaczonych przez administratora danych osobowych obszarach systemu informatycznego administratora danych;
9) **haśle** – rozumie się przez to co najmniej ośmioznakowy ciąg znaków literowych, cyfrowych, zawierający wielkie i małe litery, cyfry oraz znaki specjalne, znany jedynie osobie, której nadano identyfikator użytkownika. Pomijamy polskie znaki diaktryczne (ś, ć, ż, ź..);
10) **zasadzie czystego pulpitu** – rozumie się nie zapisywanie tworzonych dokumentów, zawierających dane, na pulpicie. Po odejściu od stanowiska, w zależności od przewidywanego czasu nieobecności, należy się wylogować i wyłączyć komputer lub zablokować dostęp do systemu operacyjnego (skrót klawiszowy: „Windows" + L);
11) **odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
    a) osoby, której dane dotyczą,
    b) osoby, upoważnionej do przetwarzania danych,
    c) przedstawiciela, o którym mowa w art. 31a ustawy,
    d) podmiotu, o którym mowa w art. 31 ustawy,
    e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
12) **serwisancie** – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego.

Rozdział 2
Poziom bezpieczeństwa

§2. 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 system informatyczny chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych i logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem. Powyższe zabezpieczenia opisane są w dalszej części instrukcji.

Rozdział 3
Nadawanie i rejestrowanie (wyrejestrowywanie) uprawnień do przetwarzania danych w systemie informatycznym

§3. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:
1) ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2016 r., poz. 922 z późn. zm.);

2) Polityką Bezpieczeństwa Informacji w Starostwie Powiatowym w Stargardzie;
3) niniejszym dokumentem,

oraz posiadać upoważnienie do przetwarzania danych osobowych.

§4. 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 Administratora Danych Osobowych (Starosty Stargardzkiego) .

§5. Administrator Systemu Informatycznego jest zobowiązany upoważnić co najmniej jednego pracownika - do rejestracji użytkowników w systemie informatycznym w czasie swojej nieobecności dłuższej niż 21 dni.

§6. Rejestracja użytkownika, polega na nadaniu unikalnego identyfikatora i przydzieleniu jednorazowego hasła (hasło podlega zmianie przez użytkownika przy pierwszym logowaniu do systemu) oraz wprowadzeniu tych danych do bazy użytkowników systemu.

§7. 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.

§8. Wyrejestrowanie, o którym mowa w §6, może mieć charakter czasowy lub trwały.

§9. Wyrejestrowanie następuje poprzez zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe) lub na czas nieokreślony

§10. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego może być:

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

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

§12. Administrator Bezpieczeństwa Informacji zobowiązany jest do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym, rejestr stanowi **załącznik nr 2**.

Rozdział 4
Metody i środki uwierzytelniania oraz procedury związane z ich zarządzeniem i użytkowaniem

§13. Identyfikator składa się z co najmniej sześciu znaków, z których pierwszy znak odpowiada pierwszej literze imienia użytkownika pisanej małą literą, a drugi znak odpowiada

pierwszej literze nazwiska pisanej małą literą i kolejne litery nazwiska pisane małymi literami. W identyfikatorze pomija się polskie znaki diakrytyczne.

§14. 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 §13.

§15. W systemie stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji.

§16. Identyfikator użytkownika w aplikacji (o ile działanie aplikacji na to pozwala), powinien być tożsamy z tym, jaki jest mu przydzielony w sieci lokalnej.

§17. Kierownicy komórek organizacyjnych zobowiązani są pisemnie informować Administratora Bezpieczeństwa Informacji o każdej zmianie dotyczącej podległych pracowników mających wpływ na zakres posiadanych uprawnień w systemie informatycznym.

§18. Bezpośredni dostęp do systemu informatycznego może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.

§19. Hasło użytkownika powinno być zmieniane nie rzadziej niż co 30 dni.

§20. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.

§21. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.

§22. Użytkownik utrzymuję swoje hasła w tajemnicy, również po upływie ich ważności.

§23. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.

§24. W sytuacji kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do zmiany hasła lub powiadomienia Administratora Systemu Informatycznego w celu przeprowadzenia procedury wymuszenia zmiany hasła.

§25. 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.

§26. 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.: „QWERTY" i „12345" itp.

§27. Zmiany hasła nie wolno zlecać innym osobom, oprócz Administratora Systemu Informatycznego, w przypadku potrzeby wymuszenia zmiany hasła.

§28. Nie należy korzystać z opcji zapamiętywania hasła w systemie.

§29. Hasła administracyjne systemów informatycznych oraz urządzeń sieci lokalnej przechowywane są w zamkniętych i zaplombowanych kopertach, w sejfie w pomieszczeniu 02 w budynku Starostwa Powiatowego w Stargardzie przy ul. Skarbowej 1. Dostęp do haseł mają wyłącznie: Starosta, Wicestarosta, Administrator Systemu Informatycznego oraz Administrator Bezpieczeństwa Informacji.

Rozdział 5
Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

§30. Rozpoczęcie pracy na stacji roboczej następuje po sprawdzeniu czy listwa zasilająca komputer i monitor włączona jest do gniazda sieciowego podłączonego do centralnego zasilacza awaryjnego (UPS). Gniazdo jest w kolorze czerwonym. Następnie włączeniu napięcia w listwie podtrzymującej napięcie (w przypadku posiadania listwy), włączeniu komputera i wprowadzeniu identyfikatora indywidualnego oraz hasła identyfikatora znanego tylko użytkownikowi. **Do gniazda oznaczonego kolorem czerwonym kategorycznie zabrania się podłączania innych urządzeń niż komputer i monitor.**

§31. W pomieszczeniu, w którym przetwarzane są dane osobowe, mogą znajdować się osoby postronne tylko za zgodą i w towarzystwie użytkownika albo Administratora Bezpieczeństwa Informacji.

§32. Przed osobami postronnymi należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwiać podgląd), wydruki leżące na biurkach oraz w otwartych szafach.

§33. W systemach operacyjnych komputerów uruchomiona jest funkcja włączająca po 5 minutach od przerwania pracy wygaszacze ekranu. Wznowienie wyświetlenia następuje dopiero po wprowadzeniu odpowiedniego hasła.

§34. W przypadku opuszczenia stanowiska pracy użytkownik obowiązany jest wylogować się z systemu lub w inny sposób aktywizować blokadę stacji roboczej.

§35. Obowiązuje zakaz robienia kopii danych. Zbiory danych mogą być kopiowane tylko przez Administratora Systemu Informatycznego lub automatycznie przez system, z zachowaniem procedur ochrony danych osobowych, w celu utworzenia kopii bezpieczeństwa lub danych archiwalnych.

§36. Jednostkowe dane mogą być przekazywane między komputerami pracującymi w sieci lokalnej a komputerami pracującymi poza siecią, tylko po ich zabezpieczeniu hasłem.

§37. Obowiązuje zakaz wynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz obszernych z nich wypisów, nawet w postaci zaszyfrowanej. Zakaz nie dotyczy kopii bezpieczeństwa i kopii archiwalnych.

§38. Przetwarzając dane osobowe, należy odpowiednio często zapisywać zmiany danych, na których się właśnie pracuje, tak aby zapobiegać ich utracie.

§39. Zakończenie pracy na stacji roboczej następuje po wprowadzeniu i zapisaniu danych programów, a następnie prawidłowym zamknięciu uruchomionych aplikacji oraz wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w listwie (jeżeli jest podłączona).

§40. Przed opuszczeniem pokoju należy:
1) zniszczyć w niszczarce lub schować do zamykanych na klucz szaf wszelkie wykonane wydruki zawierające dane osobowe;
2) schować do zamykanych na klucz szaf akta zawierające dane osobowe;
3) umieścić klucze do szaf w ustalonym, przeznaczonym do tego miejscu;
4) zamknąć okna.

§41. 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 Administratora Bezpieczeństwa Informacji lub Dyrektora Biura Obsługi Urzędu, który zgłasza osobom sprzątającym jednorazową rezygnację z wykonania usługi sprzątania.

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

§43. Użytkownicy, którym zostały powierzone komputery przenośne powinny chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych. W przypadku wykonywania obowiązków służbowych poza miejscem pracy należy zachować szczególną ostrożność podczas ich transportu. Obowiązuje całkowity zakaz wynoszenia komputerów przenośnych z pracy do domu.

§44. Obowiązuje zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone, za wyjątkiem wykonywania obowiązków służbowych.

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

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

§47. Obowiązuje zakaz przetwarzania na komputerach przenośnych całych zbiorów danych lub obszernych z nich wypisów w postaci niezaszyfrowanej.

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

§49. Komputery stacjonarne oraz przenośne wyposażone są w odpowiednie programy ochrony antywirusowej, których aktualizację pobierana jest automatyczne lub przez Administratora Systemu Informatycznego. W przypadku pojawienia się komunikatów generowanych przez program antywirusowy i dotyczących nieprawidłowej pracy programu lub wykrycia wirusów należy powiadomić Administratora Systemów Informatycznych lub Administratora Bezpieczeństwa Informacji.

Rozdział 6
Procedury tworzenia kopii zapasowych

§50. Kopie zapasowe tworzy się:

1) codziennie – w przypadku programów: PLAN B, SIGID, BESTIA, ETA, GMINA, KADRY PŁACE, STOCK;
2) raz na dwa dni – KATALOGI MOJE DOKUMENTY, FOLDERY WSPÓLNE WYDZIAŁÓW, POWIAT;
3) raz na trzy dni – KADRY PŁACE (wersja archiwalna), PŁATNIK;
4) raz w tygodniu – E-PFRON, JST+;
5) nie rzadziej niż raz na miesiąc – w przypadku kopii archiwalnych i wszystkich kopii zapasowych. Kopie na płycie BD/CD/DVD przechowywane są w zamkniętej szafie w pokoju 208 Komendy Powiatowej Państwowej Straży Pożarnej w Stargardzie, u Administratora Bezpieczeństwa Informacji.

§51. Wyżej wymienione kopie wykonywane są po zakończeniu pracy wszystkich użytkowników w sieci komputerowej.

§52. Kopia bezpieczeństwa wykonywana jest na nośniku danych o odpowiedniej pojemności.

§52. W przypadku wykonywania zabezpieczeń długoterminowych na płytach BD lub płytach CD/DVD, nośniki te należy wykonać w dwóch egzemplarzach i dwa razy w roku sprawdzać pod kątem ich dalszej przydatności.

§53. Stwierdzenie utraty przez jedną z kopii długoterminowych możliwości jej odczytu, upoważnia Administratora Systemu Informatycznego do wykonania kolejnych dwóch kopii z nośnika nieuszkodzonego i do zniszczenia dotychczas używanych nośników.

Rozdział 7
Przechowywanie elektronicznych nośników informacji zawierających dane osobowe oraz wydruków ich kopii zapasowych

§54. Elektroniczne nośniki informacji.

1. Zarejestrowane, wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych określonych w Polityce Bezpieczeństwa Informacji.

2. Po zakończeniu pracy przez użytkowników systemu, zarejestrowane, wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych.

3. 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.

4. 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.

5. 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.

§55. Zakazuje się przetwarzania danych osobowych na nośnikach zewnętrznych, oraz ich przesyłania pocztą, elektroniczną bez ich uprzedniego zaszyfrowania.

§56. Na nośnikach, o których mowa w §55 , dopuszczalne jest przetwarzanie jedynie jednostkowych danych osobowych.

§57. W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym na izolowanej przeznaczonej do tego celu stacji roboczej, która znajduje u Administratora Sieci Informatycznej. Niedopuszczalne jest bezpośrednie umieszczanie nośników zewnętrznych pochodzących od podmiotu zewnętrznego w stacji roboczej pracującej w sieci Starostwa.

§58. Nośniki zewnętrzne 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.

§59. Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione do przetwarzania danych osobowych.

§60. Nośniki do sporządzania kopii zapasowych programów, których przydatność nie nadaje się do dalszego wykorzystania są trwale niszczone.

§61. Kopie zapasowe.

1. Kopie bezpieczeństwa i kopie archiwalne są przechowywane w szafie w pokoju 218 w budynku Komendy Powiatowej Państwowej straży pożarnej przy ul. Bogusława IV 21.

2. Dostęp do danych opisanych w punkcie 1 ma: Starosta, Wicestarosta, Administrator Systemu Informatycznego, Administrator Bezpieczeństwa Informacji.

§62. 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. Pomieszczenie powinno być zamknięte, a wydruki zabezpieczone w zamkniętych szafach lub szufladach. **Zasada czystego biurka.**

3. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie. Niszczenie tych wydruków możliwe jest na stanowisku pracy wyposażonym w niszczarkę lub w pomieszczeniu 005 przez pracownika Biura Obsługi Urzędu.

Rozdział 8
Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz wirusami komputerowymi

§63. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe pracujące w trybie monitora (ciągła praca w tle).

§64. Każdy e-mail oraz załączniki muszą być sprawdzone przez program antywirusowy pod kątem obecności wirusów.

§65. Definicje wzorców wirusów aktualizowane są automatycznie, codziennie.

§66. Harmonogram zadań oprogramowania antywirusowego ma raz w tygodniu lub częściej sprawdzać daną jednostkę komputerową pod kątem obecności wirusów.

§67. Do obowiązków Administratora Systemu Informatycznego należy aktualizacja oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji wirusów dokonywanych przez to oprogramowanie.

§68. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Celem sprawdzenia takiego nośnika należy zgłosić się do Administratora Systemu Informatycznego (pokój 002), który przeprowadzi, to sprawdzenie na izolowanej stacji roboczej.

§69. Zabrania się pobierania z Internetu plików, które nie są związane z wykonywaniem obowiązków służbowych. Każdy pobrany plik musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.

§70. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.

§71. Zabrania się otwierania nieznanych łączy zawartych w poczcie elektronicznej bez wcześniejszej konsultacji z Administratorem Systemu Informatycznego.

§72. Administrator Systemu Informatycznego przeprowadza cyklicznie kontrole antywirusowe na wszystkich komputerach – minimum co trzy miesiące.

§73. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku stwierdzenia nieprawidłowości zgłoszonych przez pracownika w funkcjonowaniu sprzętu komputerowego lub oprogramowania.

§74. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe na którym wykryto wirusa oraz wszystkie posiadane przez użytkownika nośniki.

§75. Użytkownik jest obowiązany zawiadomić administratora systemu informatycznego o pojawiających komunikatach wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.

Rozdział 9
Kontrola nad wprowadzaniem, dalszym przetwarzaniem i udostępnianiem danych osobowych

§76. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom uprawnionym, zgodnie z przepisami prawa.

§77. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną.

Rozdział 10
Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

§78. Przeglądu i konserwacji systemu dokonuje administrator systemu informatycznego doraźnie.

§79. Przeglądu i konserwacji urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonych przez producenta sprzętu.

§80. 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.

§81. Przeglądu pliku zawierającego raport dotyczący działalność aplikacji bądź systemów serwerowych (log systemowy) Administrator Systemu Informatycznego dokonuje nie rzadziej niż raz na miesiąc.

§82. W przypadku działań konserwacyjnych, awarii oraz napraw Administrator Bezpieczeństwa Informacji prowadzi „Dziennik systemu informatycznego Starostwa Powiatowego w Stargardzie **załącznik nr 3.**

§83. Wpisów do dziennika może dokonywać Administrator Danych, Administrator Bezpieczeństwa Informacji lub Administrator Systemu Informatycznego.

Rozdział 11
Naprawa urządzeń komputerowych z chronionymi danymi osobowymi

§84. Wszelkie naprawy urządzeń komputerowych oraz zmiany w systemie informatycznym Administratora Danych przeprowadzane są - jeżeli jest to możliwe - przez Administratora Systemu Informatycznego.

§85. Naprawy i zmiany w systemie informatycznym Administratora Danych przeprowadzane przez serwisanta prowadzone są pod nadzorem Administratora Systemu Informatycznego, 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.

Rozdział 12
Postanowienia końcowe

§86. W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.

§87. 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.

STAROSTA
Iwona Wiśniewska

Załącznik nr 1
do Instrukcji Zarządzania
Systemem Informatycznym

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 Informatycznego:	Akceptacja ABI

STAROSTA
Iwona Wiśniewska

Załącznik nr 2
do Instrukcji Zarządzania Systemem Informatycznym

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

Lp.	Nazwisko, Imię	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania uprawnień	Data ustania uprawnień	Identyfikator użytkownika	Uwagi

STAROSTA
Iwona Wiśniewska

Załącznik nr 3
do Instrukcji Zarządzania
Systemem Informatycznym

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 STARGARDZIE

Lp.	Data i godzina zdarzenia	Opis zdarzenia	Podjęte działania/wnioski	Podpis

STAROSTA
Iwona Wiśniewska

Załącznik nr 5
Do Polityki
Bezpieczeństwa Informacji

Instrukcja postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych

§1. Postanowienia ogólne:

1. Niniejsza instrukcja obejmuje wszystkie obszary Starostwa Powiatowego w Stargardzie, w których przetwarzane są dane osobowe.

2. Do stosowania niniejszej instrukcji obowiązani są wszyscy pracownicy Starostwa Powiatowego w Stargardzie, upoważnieni do przetwarzania danych osobowych, na podstawie pisemnego upoważnienia.

§ 2. Celem instrukcji jest ustalenie jednolitych zasad postępowania w przypadku, gdy:

1) stwierdzono naruszenie lub istnieje podejrzenie naruszenia ochrony danych osobowych, zgromadzonych w systemach informatycznych lub na innych nośnikach informacji, w tym nośnikach papierowych;
2) stan urządzenia, zawartość zbioru danych osobowych, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zasad ochrony danych.

§ 3. Naruszenie ochrony danych osobowych może być skutkiem:

1) szkodliwego wpływu środowiska na system przetwarzania danych osobowych;
2) zewnętrznych zdarzeń losowych;
3) zamierzonych lub niezamierzonych czynności użytkowników systemów przetwarzania danych osobowych;
4) nieuprawnionych działań osób nieupoważnionych do dostępu do danych osobowych.

§ 4. Za naruszenie zasad ochrony danych osobowych uważa się w szczególności:

1) nieupoważniony dostęp, modyfikację, kopiowanie lub zniszczenie/usunięcie danych osobowych, zarówno w systemie informatycznym, jak i na nośnikach papierowych oraz elektronicznych;
2) udostępnianie danych osobowych nieuprawnionym podmiotom lub osobom;
3) nieautoryzowany dostęp do danych przez połączenie sieciowe;
4) nieautoryzowany dostęp do pomieszczeń, w których przetwarza się dane osobowe;
5) niedopełnienie obowiązku ochrony danych osobowych przez umożliwienie dostępu do danych (np. pozostawienie kopii danych, niezablokowanie dostępu do systemu, brak nadzoru nad serwisantami i innymi osobami nieuprawnionymi przebywającymi w pomieszczeniach gdzie przetwarza się dane osobowe;
6) wykrycie niezabezpieczonego kanału dystrybucji danych osobowych;
7) nielegalne bądź nieświadome ujawnienie danych osobowych;
8) pozyskiwanie danych osobowych z nielegalnych źródeł;
9) przetwarzanie danych osobowych niezgodne z uprawnionym celem i zakresem;
10) stwierdzenie obecności wirusów komputerowych lub innych programów godzących w integralność systemu informatycznego;

11) ujawnienie indywidualnych haseł dostępu do danych osobowych w systemie;
12) przesyłanie danych osobowych przez Internet bez zabezpieczenia;
13) przesyłanie dokumentów papierowych i nośników elektronicznych z danymi bez zabezpieczenia;
14) wykonanie nieuprawnionych kopii danych osobowych;
15) naruszenie bezpieczeństwa kopii danych osobowych;
16) kradzież nośników zawierających dane osobowe lub oprogramowanie;
17) kradzież sprzętu służącego do przetwarzania danych osobowych;
18) utratę danych osobowych w systemie informatycznym, na kopiach bezpieczeństwa i na innych nośnikach;
19) brak aktualnych kopii bezpieczeństwa danych osobowych lub brak odpowiednich nośników do sporządzania kopii;
20) niewłaściwe niszczenie nośników z danymi osobowymi pozwalające na ich odczyt;
21) naruszenie zasad ochrony fizycznej pomieszczeń, w których przetwarza się dane osobowe;
22) dopuszczenie do przetwarzania danych osobowych pracowników bez odpowiednich upoważnień;
23) nie przeszkolenie pracowników w zakresie bezpieczeństwa danych osobowych;
24) inne sytuacje wskazujące lub potwierdzające naruszenie bezpieczeństwa danych osobowych w Starostwie Powiatowym w Stargardzie.

§ 5. O możliwości zaistnienia przypadku naruszenia zasad ochrony danych osobowych mogą świadczyć m.in.:
1) nadmierne, w stosunku do wykonywanych zadań (zakres upoważnienia), uprawnienia użytkownika do zasobów systemu;
2) niestabilna praca systemu, w którym przetwarza się dane osobowe;
3) korzystanie z zasobów systemu poza godzinami pracy (bez zgody przełożonego);
4) nowe „podejrzane" konta użytkowników;
5) wysoka aktywność kont, które długo pozostawały niewykorzystane;
6) zanotowanie w krótkim czasie dużej liczby nieudanych prób logowania (zakładamy jednakże, że system jest tak skonfigurowany, iż po trzech próbach podania błędnego hasła wymaga interwencji administratora);
7) anomalie w pracy systemu lub programu (świadczące np. o obecności wirusa);
8) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach, w których przetwarza się dane osobowe (wyłamane lub zacinające się zamki, naruszone plomby, niedomykające się okna itp.).

§ 6. Osoba, która podejrzewa lub stwierdzi naruszenie zasad ochrony danych osobowych ma obowiązek niezwłocznie (bezpośrednio lub telefonicznie):
1) powiadomić o zaistniałym zdarzeniu Administratora Bezpieczeństwa Informacji oraz swojego bezpośredniego przełożonego;
2) określić (opisać) symptomy świadczące o możliwości naruszenia lub naruszeniu zasad ochrony danych;
3) określić sytuację i czas w jakim je zauważono;
4) podać wszelkie istotne informacje mogące pomóc w ustaleniu przyczyny naruszenia zasad ochrony danych osobowych;

5) nie podejmować dalszej pracy w systemie informatycznym bez decyzji Administratora Bezpieczeństwa Informacji.

§7. Administrator Bezpieczeństwa Informacji ocenia sytuację i podejmuje odpowiednie do potrzeb działania, a w szczególności:

1) dokonuje rozpoznania zdarzenia;
2) ocenia wagę problemu;
3) ocenia możliwość wystąpienia strat w zasobach informacyjnych i systemowych w przypadku dalszego działania systemu;
4) lokalizuje źródło problemu (przeprowadza analizę posiadanych danych).

§8. W przypadku stwierdzenia, że podejrzenie nie świadczy o naruszeniu zasad ochrony danych, Administrator Bezpieczeństwa Informacji po przeanalizowaniu sytuacji i wyeliminowaniu możliwości wystąpienia ich w przyszłości, podejmuje decyzję o dalszej pracy systemu.

§9. Każda interwencja Administratora Bezpieczeństwa Informacji kończy się niezwłoczną analizą postępowania i sporządzeniem raportu.

§10. Jeżeli w czasie usuwania skutków naruszenia bezpieczeństwa danych osobowych nastąpi czasowe obniżenie poziomu bezpieczeństwa systemu, po zakończeniu czynności naprawczych, system przetwarzający te dane powinien posiadać poziom bezpieczeństwa nie niższy niż poprzedni.

§11. Każda informacja o naruszeniu ochrony danych i jego okolicznościach, kierowana poza Starostwo Powiatowe w Stargardzie, może być przekazana wyłącznie przez Administratora Danych Osobowych.

§12. Każda osoba dopuszczona do przetwarzania danych osobowych obowiązana jest zapoznać się z niniejszą Instrukcją oraz złożyć stosowne oświadczenie dotyczące znajomości wymienionych regulacji.

§13. Osoba upoważniona do przetwarzania danych osobowych za naruszenie obowiązków, wynikających z niniejszej Instrukcji i przepisów o ochronie danych osobowych ponosi odpowiedzialność przewidzianą w Regulaminie Pracy oraz Kodeksie Pracy (Dz. U. z 2016 r. poz. 1666) za ciężkie naruszenie podstawowych obowiązków pracowniczych oraz odpowiedzialność karną zgodnie z ustawą o ochronie danych osobowych.

STAROSTA
Iwona Wiśniewska

Załącznik nr 6
Do Polityki
Bezpieczeństwa Informacji

Zgoda na przetwarzanie danych osobowych

Ja, niżej podpisana/ny wyrażam zgodę na przetwarzanie moich danych osobowych w podanym wyżej/niżej zakresie

.....

.....

(zakres przetwarzanych danych powinien być zdefiniowany, jeżeli nie wynika wprost z formularza, pod którym zgoda jest zamieszczona)

przez.....

(nazwa administratora danych i jego adres)

w celach .....

(cel przetwarzania danych np. w celach rekrutacyjnych)

Zgodnie z art. 23 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r. poz. 922 z późn. zm.).

.....

Data, miejsce i podpis osoby wyrażającej zgodę*

* Jeżeli zgoda wyrażana jest elektronicznie, system informatyczny powinien przechowywać informacje na temat wyrażenia zgody.

STAROSTA
Iwona Wiśniewska

Załącznik nr 7
Do Polityki
Bezpieczeństwa Informacji

Data nadania upoważnienia:..... .

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Nr .....

1. Na podstawie art. 37 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r. poz. 922 z późn. zm.)

u p o w a ż n i a m

Pana/Panią ..... , pracownika .....
w Wydziale ..... w Starostwie Powiatowym w Stargardzie,
do **przetwarzania danych osobowych w systemie informatycznym** .....
oraz w systemie nieinformatycznym Starostwa Powiatowego w Stargardzie w granicach nieprzekraczających ustalonego zakresu obowiązków.

2. Osoba upoważniona do przetwarzania danych posługuje się identyfikatorem dostępu do systemu informatycznego, który wyrażony jest słowem „.....".
3. Upoważnienie obowiązuje **od** ..... **do** .....
4. Osoba upoważniona do przetwarzania danych jest zobowiązana po ustaniu umowy o pracę do:
   a) zachowania w tajemnicy danych, z którymi miała do czynienia w czasie wykonywania obowiązków służbowych,
   b) zachowania w tajemnicy informacji o zabezpieczeniu danych.

.....
(podpis administratora danych)

....
(Data i podpis osoby upoważnionej)

STAROSTA
Iwona Wiśniewska

Załącznik nr 8
Do Polityki
Bezpieczeństwa Informacji

Stargard dn. .....

.....
imię i nazwisko

.....
stanowisko

.....
wydział/Biuro

OŚWIADCZENIE

Oświadczam, iż zostałam/em zapoznana/y z przepisami dotyczącymi ochrony danych osobowych, a w szczególności ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 z późn. zm), wydanymi na jej podstawie aktami wykonawczymi oraz wprowadzonymi i wdrożonymi do stosowania przez Administratora Danych Osobowych „Polityką Bezpieczeństwa Informacji" oraz „ Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" w Starostwie Powiatowym w Stargardzie.

Zobowiązuję się do:

1) zachowania w tajemnicy danych osobowych, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań służbowych lub obowiązków pracowniczych;
2) niewykorzystywania danych osobowych w celach pozasłużbowych;
3) zachowania w tajemnicy sposobów zabezpieczenia danych osobowych;
4) korzystania ze sprzętu IT oraz oprogramowania wyłącznie związku z wykonywaniem obowiązków pracowniczych;
5) wykorzystywania tylko legalnego oprogramowania pochodzącego od Pracodawcy;
6) należytej dbałości o sprzęt i oprogramowanie zgodnie z dokumentacją ochrony danych osobowych.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane przez Pracodawcę za ciężkie naruszenie obowiązków pracowniczych w rozumieniu art. 52 §1 pkt 1 Kodeksu Pracy lub za naruszenie przepisów karnych ww. ustawy o ochronie danych osobowych.

.....
podpis pracownika

Stargard dn. .....

.....
imię i nazwisko

.....
adres

OŚWIADCZENIE

Oświadczam, że zobowiązuję się zarówno w trakcie umowy jak i po jej ustaniu do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia do których będę miał/ła dostęp, w związku z wykonywaniem zapisów umowy. Oświadczam, że zostałam/em zapoznana/y z przepisami dotyczącymi ochrony danych osobowych, a w szczególności ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 z późn. zm), wydanymi na jej podstawie aktami wykonawczymi oraz wprowadzonymi i wdrożonymi do stosowania przez Administratora Danych Osobowych „Polityką Bezpieczeństwa Informacji". Przyjmuję do wiadomości, że postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane przez Pracodawcę za ciężkie naruszenie obowiązków pracowniczych w rozumieniu art. 52 §1 pkt 1 Kodeksu Pracy lub za naruszenie przepisów karnych ww. ustawy o ochronie danych osobowych.

.....
podpis pracownika

STAROSTA
Iwona Wiśniewska

Załącznik nr 9
Do Polityki
Bezpieczeństwa Informacji

Instrukcja zarządzania kluczami w Starostwie Powiatowym w Stargardzie

§1. Postanowienia ogólne

1. Niniejsza instrukcja reguluje sposób pobierania, zdawania i przechowywania kluczy do pomieszczeń w Starostwie Powiatowym w Stargardzie.

2. Wszystkie klucze do pomieszczeń wraz z kluczami zapasowymi oznaczone są numerem i przechowywane w zamykanej na klucz szafce, przy stanowisku pracy ochrony Urzędu.

3. Zabrania się zabierania kluczy poza teren Urzędu.

4. O utracie, uszkodzeniu lub zniszczeniu klucza użytkownik niezwłocznie powiadamia Dyrektora Biura Obsługi Urzędu oraz Administratora Bezpieczeństwa Informacji.

5. Od momentu pobrania klucza do momentu jego zdania, na pracownikach spoczywa pełna odpowiedzialność za zabezpieczenie udostępnionych im pomieszczeń.

§2. Tryb postępowania przy wydawaniu kluczy

1. Po podpisaniu listy obecności przez pracownika, pracownik ochrony wydaje klucze do pomieszczenia, w którym pracownik pracuje.

2. Po zakończeniu pracy pracownik, który pobrał klucz zobowiązany jest go zwrócić pracownikowi ochrony. Pracownik ochrony sprawdza, czy wszystkie wydane klucze zostały zwrócone i odnotowuje ten fakt w raporcie dziennym. W przypadku stwierdzenia nieoddania klucza, pracownik ochrony zobowiązany jest do bezzwłocznego wyjaśnienia zaistniałego zdarzenia, a w przypadku bezskuteczności podjętych działań sprawdza zabezpieczenie pomieszczenia, sporządza notatkę z zaistniałego zdarzenia i powiadamia Dyrektora Biura Obsługi Urzędu i Administratora Bezpieczeństwa Informacji.

3. Każdorazowe wydanie pracownikowi klucza, po godzinach pracy oraz wydanie klucza zapasowego, pracownik ochrony ma obowiązek odnotować w raporcie dziennym, wpisując: nr klucza, imię i nazwisko osoby pobierającej, datę i godzinę wydania oraz zdania klucza.

4. Wydanie kluczy w dni świąteczne i wolne od pracy może nastąpić tylko w przypadku wydania zgody przez Starostę, Sekretarza Powiatu i Dyrektora Biura Obsługi Zarządu i Rady Powiatu, na przebywanie w Urzędzie po godzinach pracy oraz w dni świąteczne i wolne od pracy.

§3. Wydawanie kluczy osobom sprzątającym - tryb przyjmowania, przechowywania i wydawania kluczy osobom sprzątającym:

1) klucze przydzielone osobom sprzątającym są kluczami zapasowymi;
2) wydawanie i przyjęcie kluczy od osoby sprzątającej następuje po odnotowaniu tego faktu, przez pracownika ochrony, w raporcie dziennym;
3) pracownik ochrony sprawdza czy zdano wszystkie klucze. W przypadku stwierdzenia braku kluczy bezzwłocznie wyjaśnia zaistniałe zdarzenie. W przypadku bezskuteczności podjętych działań ww. pracownik sprawdza zabezpieczenie pomieszczeń sporządza notatkę z zaistniałego zdarzenia oraz powiadamia Dyrektora Biura Obsługi Urzędu i Administratora Bezpieczeństwa Informacji.

§4. Postanowienia końcowe.

1. W przypadkach, kiedy wydanie klucza jest niezbędne dla zapewnienia bezpieczeństwa mienia znajdującego się w pomieszczeniach, pracownik ochrony bezzwłocznie wydaje klucz, odnotowując w raporcie dziennym, godzinę wydania i zdania, nr klucza oraz imię i nazwisko osoby, której wydał klucz.

2. Nieprzestrzeganie opisanych w niniejszej instrukcji procedur, zgodnie z Polityką Bezpieczeństwa Informacji stanowi zdarzenie naruszające system ochrony danych oraz powoduje odpowiedzialność porządkową pracowników.

STAROSTA
Iwona Wiśniewska

Załącznik nr 10
Do Polityki
Bezpieczeństwa Informacji

Wzór umowy powierzenia przetwarzania danych osobowych
Umowa Nr .....

Zawarta w dniu ..... r. w .....

pomiędzy:

..... – Starostą Stargardzkim (Administratorem Danych Osobowych), ul. Skarbowa 1, 73-110 Stargard zwanym w dalszej części niniejszej umowy „Zleceniodawcą"

a

.....
zwanym w dalszej części niniejszej umowy „Przetwarzającym"
reprezentowanym przez:
.....
-wspólnie zwanymi dalej „Stronami"

§ 1

1. Użyte w umowie określenia oznaczają:
   1) **ustawa** – ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;
   2) **rozporządzenie** – rozporządzenie Ministra Spraw 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;
   3) **dane osobowe** – dane osobowe w rozumieniu art. 6 ustawy, przetwarzane w systemie, w celu realizacji umowy;
   4) **przetwarzanie danych** – jakiekolwiek operacje wykonywane na danych, takie jak gromadzenie, utrwalanie, modyfikacja, usuwanie, przechowywanie, przenoszenie i przekazywanie, które wykonuje się w systemie informatycznym .....;
   5) **dokument** – dowolny nośnik, tradycyjny lub elektroniczny, na którym zapisane są dane osobowe;
   6) **pracownik** – osobę świadczącą pracę na podstawie stosunku pracy lub stosunku cywilnoprawnego.

§ 2

1. Zleceniodawca oświadcza, że jest Administratorem Danych, które powierza.

2. Na podstawie art. 31 ustawy Zleceniodawca (Administrator Danych) powierza Przetwarzającemu, przetwarzanie danych osobowych w imieniu i na rzecz Zleceniodawcy (Administratora Danych), na warunkach opisanych w niniejszej umowie.

§ 3

1. Przetwarzający będzie przetwarzał, powierzone na podstawie niniejszej Umowy, następujące zbiory danych osobowych:
   1) dane osobowe osób..... , obejmujące imię, nazwisko, numer ewidencyjny PESEL, ...;
   2) dane osobowe osób..... , obejmujące imię, nazwisko, numer ewidencyjny PESEL, ... ;
   3) .....

§ 4

1. Przetwarzający upoważni swoich pracowników do przetwarzania danych osobowych. Przetwarzający ograniczy dostęp do przetwarzania danych osobowych wyłącznie do pracowników posiadających upoważnienia do przetwarzania tych danych.

2. Zleceniodawca (Administrator Danych) dopuszcza stosowanie przez przetwarzającego wzoru upoważnienia do przetwarzania danych osobowych, stanowiącego załącznik do polityki Bezpieczeństwa Informacji Przetwarzającego.

3. Przetwarzający powierzy, za zgodą Zleceniodawcy, przetwarzanie danych osobowych w zakresie wykonywania usług serwisowych, Wykonawcy każdorazowo wyłonionemu przez Przetwarzającego, w ramach przepisów – Ustawy o zamówieniach publicznych.

4. W celu zapewnienia maksymalnego poziomu bezpieczeństwa przetwarzania danych osobowych powierzenie i jego warunki, o których mowa w ust. 3 zostaną określone w odrębnej umowie

§5

1. Przetwarzający zapewni środki techniczne i organizacyjne należytego zabezpieczenia danych osobowych, wymagane przepisami prawa, w tym w szczególności art. 36 ustawy oraz rozporządzenia.

2. Przetwarzający w szczególności:
   1) będzie prowadził dokumentację opisującą sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych, w tym w szczególności politykę bezpieczeństwa informacji oraz instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych;
   2) dopuści do przetwarzania danych osobowych wyłącznie osoby posiadające upoważnienie, o którym mowa w §4 ust. 1;
   3) będzie prowadzić ewidencję pracowników upoważnionych do przetwarzania danych osobowych;
   4) spełni warunki techniczne i organizacyjne, którym odpowiadać powinny urządzenia i systemy informatyczne stosowane do przetwarzania danych osobowych, określone w rozporządzeniu;

5) będzie wymagał od swoich pracowników przestrzegania należytej staranności w zakresie zachowania w poufności danych osobowych oraz ich zabezpieczenia, także po ustaniu zatrudnienia u Przetwarzającego;
6) zobowiązuje się nie wykorzystywać zebrane dane osobowe do celów innych niż określone w umowie.

§ 6

1. Umowę zawiera się na czas nieoznaczony/określony do dnia ..... .

2. Zleceniodawca ma prawo rozwiązać niniejszą Umowę, w szczególności gdy Przetwarzający:
   1) wykorzystał dane osobowe w sposób niezgodny z niniejszą Umową;
   2) powierzył przetwarzanie danych osobowych podwykonawcom bez zgody Zleceniodawcy;
   3) nie zaprzestanie niewłaściwego przetwarzania danych osobowych;
   4) zawiadomi o swojej niezdolności do dalszego wykonywania niniejszej Umowy, a w szczególności niespełniania wymagań określonych w §3.

3. Wypowiedzenie umowy może nastąpić w każdym czasie na wniosek jednej ze stron.

4. Po rozwiązaniu lub wygaśnięciu umowy, Przetwarzający niezwłocznie, ale nie później niż w terminie do 5 dni kalendarzowych, zobowiązuje się zwrócić lub usunąć wszelkie dane osobowe, których przetwarzanie zostało mu powierzone, w tym skutecznie usunąć je również z nośników elektronicznych pozostających w jego dyspozycji i potwierdzić powyższe przekazanym Zleceniodawcy protokołem.

5.W przypadku nie wywiązania się Przetwarzającego z obowiązków wynikających z niniejszej umowy w szczególności z określonych w ust. 4, Zleceniodawca ma prawo zawiadomić o uchybieniach GIODO oraz organy ścigania.

§ 7

W sprawach nieuregulowanych niniejszą umową zastosowanie maja przepisy prawa, a w szczególności ustawa z dnia 23 kwietnia 1964r. Kodeks cywilny (Dz. U. z 2015 r. poz. 2164 z późn. zm) oraz ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. 2016 r. poz. 922 z późn. zm.)

§8

Wszelkie zmiany lub uzupełnienia niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.

§9

Umowę sporządzono w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze stron.

....

Zleceniodawca Przetwarzający

52 STAROSTA Iwona Wiśniewska