ZARZĄDZENIE NR 17/2016

STAROSTY ŁOWICKIEGO

z dnia 21 marca 2016r.

w sprawie wprowadzenia dokumentacji zapewniającej ochronę przetwarzania danych osobowych w Starostwie Powiatowym w Łowiczu wraz z opisem środków technicznych i organizacyjnych stosowanych w jednostce.

Na podstawie art. 36 ust. 2 ustawy z dnia z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2015 r. poz. 2135), Rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z dnia 29 kwietnia 2004 r. (Dz. U. Nr 100, poz. 1024) oraz art. 34 ust. 1 i art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 roku o samorządzie powiatowym (t.j. Dz. U. z 2015 r. poz. 1445;1890) zarządzam, co następuje:

§1. Wprowadzam *Politykę Bezpieczeństwa przetwarzania danych osobowych w Starostwie Powiatowym w Łowiczu*, stanowiącą załącznik nr 1 do niniejszego zarządzenia.

§2. Wprowadzam *Instrukcję zarządzania systemem informatycznym do przetwarzania danych osobowych,* stanowiącą załącznik nr 2 do niniejszego zarządzenia .

§3. Administratorem Bezpieczeństwa Informacji (ABI) w Starostwie Powiatowym w Łowiczu jest pracownik wyznaczony odrębnym zarządzeniem.

§4. Administratorem Systemów Informatycznych (ASI) służących do przetwarzania danych osobowych w Starostwie Powiatowym w Łowiczu jest pracownik wyznaczony odrębnym zarządzeniem.

§5. Nadzór nad wykonaniem zarządzenia powierzam Sekretarzowi Powiatu Łowickiego.

§6. Traci moc Zarządzenie Starosty Łowickiego nr 26/2012 z dnia 09 października 2012 roku w sprawie wprowadzenia Polityki bezpieczeństwa w zakresie przetwarzania danych osobowych i Instrukcji zarządzania systemem informatycznym do przetwarzania danych osobowych.

§7. Zarządzenie wchodzi w życie z dniem 04 kwietnia 2016 r.

STAROSTA ŁOWICKI

Krzysztof Figat

RADCA PRAWNY

Uzasadnienie:

Niniejsze zarządzenie tworzy dokumentację przetwarzania danych osobowych, której celem jest zapewnienie należytej ochrony danych osobowych będących w zasobach Starostwa Powiatowego w Łowiczu przez administratora danych, w szczególności odpowiedniej do zagrożeń i kategorii danych osobowych objętych ochroną.

Jest to podstawa do przygotowania procedur wewnętrznych, metod zarządzania i wymagań niezbędnych dla zapewnienia adekwatnych i proporcjonalnych zabezpieczeń, właściwej ochrony informacji posiadanych i administrowanych przez Starostwo Powiatowe oraz wykorzystywanych do przetwarzania danych w systemach informatycznych, przy uwzględnieniu występującego ryzyka związanego z zagrożeniami, takimi jak: działalność przestępcza, błędy i nieprawidłowości w postępowaniu pracowników, przerwy i zakłócenia w działaniu systemu.
Bezpieczeństwo danych osobowych przetwarzanych w Starostwie Powiatowym w Łowiczu jest przedmiotem szczególnej troski Starosty Łowickiego i wszelkie naruszenia ustanowionych zasad bezpieczeństwa będą spotykać się ze zdecydowaną reakcją przewidzianą w procedurach prawnych. Żadne odstępstwa od zasad bezpieczeństwa przedstawionych w przedmiotowym dokumencie są niedopuszczalne.

Zakres przedmiotowy stosowania niniejszej dokumentacji obejmuje wszystkie zbiory danych osobowych przetwarzane przez administratora danych, zarówno w formie elektronicznej, jak i papierowej, oraz dane osobowe przetwarzane poza zbiorami danych.

Zakres podmiotowy stosowania niniejszej dokumentacji obejmuje wszystkich pracowników oraz osoby, przy pomocy których administrator danych wykonuje swoje czynności, mające dostęp do danych osobowych.

Załącznik nr 1
do Zarządzenia nr 17/2016
Starosty Łowickiego
z dnia 21 marca 2016 roku

POLITYKA BEZPIECZEŃSTWA
przetwarzania danych osobowych
w
Starostwie Powiatowym w Łowiczu

Marzec 2016 r.

SPIS TREŚCI

DEFINICJE 3
POSTANOWIENIA OGÓLNE 4
ADMINISTRATOR 5
ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI I ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH 6
PRZETWARZANIE DANYCH 7
POWIERZENIE PRZETWARZANIA DANYCH 8
WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH 8
OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I POWIĄZANIA POMIĘDZY NIMI 9
SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI 9
REJESTR ZBIORÓW DANYCH OSOBOWYCH PROWADZONY PRZEZ ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI 10
OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH 10
EWIDENCJA OSÓB UPOWAŻNIONYCH 12
SZKOLENIA 12
WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ TWORZĄCYCH OBSZAR W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE 13
OKREŚLENIE ŚRODKÓW TECHNICZNYCH ORGANIZACYJNYCH NIEZBĘDNNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH 13
POSTĘPOWANIE W RAZIE ZAISTNIENIA ZAGROŻENIA DLA BEZPIECZEŃSTWA PRZETWARZANYCH DANYCH OSOBOWYCH LUB NARUSZENIA ZASAD PRZETWARZANIA DANYCH OSOBOWYCH 15
POSTANOWIENIA KOŃCOWE 15

DEFINICJE

§1. Użyte w niniejszej dokumentacji przetwarzania danych osobowych definicje i pojęcia są wspólne dla wszystkich dokumentów powiązanych z niniejszą dokumentacją oraz dla wszystkich pozostałych dokumentów, które zostały przyjęte przez Administratora w zakresie ochrony danych osobowych. Ilekroć w niniejszej polityce bezpieczeństwa jest mowa o:

1) **Administratorze danych** – rozumie się przez to Starostę Łowickiego, który decyduje o celach i środkach przetwarzania danych osobowych w Starostwie Powiatowym w Łowiczu, dalej zwanego „Administratorem";
2) **Administratorze bezpieczeństwa informacji (lub „ABI")** – rozumie się przez to osobę, wyznaczoną przez Administratora oddzielnym zarządzeniem, która jest odpowiedzialna za zapewnienie przetwarzania danych zgodnie z odpowiednimi przepisami ustawy i rozporządzenia;
3) **Administratorze systemów informatycznych (lub „ASI")** – rozumie się przez to osobę, wyznaczoną przez Administratora oddzielnym zarządzeniem, która odpowiada za zapewnienie sprawności, należytej konserwacji i wdrażania technicznych zabezpieczeń systemów informatycznych oraz odpowiada za to, aby systemy informatyczne, w których przetwarzane są dane osobowe spełniały wymagania przewidziane ustawą i rozporządzeniem;
4) **Danych osobowych (lub „dane")** – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
5) **Dokumentacji przetwarzania danych osobowych** – rozumie się przez to politykę bezpieczeństwa przetwarzania danych osobowych i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
6) **Generalnym Inspektorze Ochrony Danych Osobowych (GIODO)** – rozumie się przez to organ ochrony danych osobowych, zwany dalej **„Generalnym Inspektorem";**
7) **Identyfikatorze (loginie) użytkownika** — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
8) **Osobie fizycznej możliwej do zidentyfikowania** – rozumie się przez to osobę, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności poprzez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne; informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań;
9) **Upoważnieniu** – rozumie się przez to oświadczenie nadawane przez Administratora wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym oświadczeniu;
10) **Osobie upoważnionej** – rozumie się przez to osobę, która otrzymała od Administratora upoważnienie do przetwarzania danych;
11) **Kierowniku** – rozumie się przez to bezpośredniego przełożonego osób zatrudnionych w biurze/wydziale/samodzielnym stanowisku w Starostwie Powiatowym w Łowiczu;
12) **Przetwarzaniu danych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, które wykonuje się w systemach informatycznych oraz wersji papierowej;

13) **Rozporządzeniu** – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (Dz.U. Nr 100, poz. 1024) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;

14) **Ustawie** – rozumie się przez to ustawę z dnia z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2015 r. poz. 2135 z dnia 2015-12-16);

15) **Użytkownik uprzywilejowany** – należy przez to rozumieć osobę upoważnioną, posiadającą nadane uprawnienia na poziomie administratora systemu informatycznego;

16) **Użytkowniku systemu** – rozumie się przez to osobę upoważnioną, która otrzymała dostęp do sieci LAN umożliwiający korzystanie z sieci Internet oraz login i hasło do systemu;

17) **Załącznikach** – rozumie się przez to wzory dokumentów; Administrator może przedmiotowe wzory zastąpić wydrukami z systemów komputerowych lub innymi dokumentami o treści zgodnej z przepisami powszechnie obowiązującego prawa;

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

POSTANOWIENIA OGÓLNE

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, ABI, ASI.
Do wiadomości: Osoby upoważnione.

§2.1. W celu zapewnienia ochrony przetwarzanych danych osobowych zarówno za pomocą systemów informatycznych jak i w wersji papierowej Administrator wdraża niniejszą politykę bezpieczeństwa wraz z instrukcją zarządzania systemem informatycznym.

2. Administrator dokłada należytej staranności w celu ochrony interesów osób, których dane osobowe dotyczą, w szczególności jest obowiązany zapewnić, aby dane: były przetwarzane zgodnie z prawem, zbierane dla oznaczonych celów, merytorycznie poprawne i adekwatne do celów w jakich są zbierane, przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą oraz aby zapewniona była rozliczalność, integralność i poufność danych, gdzie przez:

1) **rozliczalność** - rozumie się właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
2) **integralność danych** - rozumie się właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
3) **poufność danych** - rozumie się właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym podmiotom.

3. Administrator deklaruje pełne zaangażowanie i determinację celem zapewnienia bezpieczeństwa przetwarzanych danych osobowych, a także prawidłowego zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych.

4. Administrator nadzoruje jakie dane, kiedy i przez kogo zostały do zbiorów Administratora wprowadzone, bądź z tych zbiorów usunięte oraz komu są przekazywane.

5. Administrator na bieżąco dostosowuje systemy informatyczne służące do przetwarzania danych i wszelkie systemy zabezpieczeń przetwarzania danych osobowych do wymogów określonych w rozporządzeniu.

§3.1. Polityka bezpieczeństwa jest dokumentem wewnętrznym i nie może być udostępniana podmiotom trzecim bez uprzedniej zgody Administratora.

2. Dla codziennych potrzeb pracowników i współpracowników Administrator odrębnym zarządzeniem wprowadzi ***Regulamin ochrony danych osobowych w Starostwie Powiatowym w Łowiczu,*** zawierający zasady przetwarzania danych osobowych obowiązujące w Starostwie.

3. Regulamin jest jawny i udostępniany w sposób powszechnie przyjęty u Administratora wszystkim pracownikom i współpracownikom.

ADMINISTRATOR

Zakres przedmiotowy stosowania: Podmioty obowiązane do stosowania: Administrator, ABI, ASI. Do wiadomości: Osoby upoważnione.

§4.1. Administrator stosuje środki techniczne i organizacyjne zapewniające ochronę danych osobowych odpowiednią do zagrożeń oraz kategorii przetwarzanych danych oraz zabezpiecza posiadane dane przed: ich udostępnieniem, zmianą, utratą, uszkodzeniem, zniszczeniem lub przetwarzaniem przez osobę nieupoważnioną.

2. Administrator w szczególności zapewnia:

1) **środki techniczne i organizacyjne** niezbędne dla zapewnienia bezpiecznego przetwarzania danych w pomieszczeniach do tego przeznaczonych;
2) **system i sprzęt informatyczny** umożliwiający bezpieczne przetwarzanie danych;
3) **że do przetwarzania danych osobowych** zostały dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych; szkolenie z zakresu ochrony danych osobowych każdej osoby przetwarzającej dane osobowe przed nadaniem jej upoważnienia i dopuszczeniem do przetwarzania danych;
4) **prowadzenie ewidencji osób upoważnionych;**
5) **należyte i terminowe udzielanie informacji** na wniosek osób, których dane są przetwarzane i które zwróciły się z wnioskiem o udzielenie informacji w trybie art. 33 ustawy;
6) **kontrolę nad tym jakie dane**, kiedy i przez kogo zostały do zbiorów Administratora wprowadzone, ze zbiorów usunięte oraz komu i przez kogo przekazane.

3. Do obowiązków Administratora należy także zarejestrowanie zbiorów danych osobowych podlegających rejestracji, w rejestrze prowadzonym przez Generalnego Inspektora Ochrony Danych Osobowych, w jego imieniu obowiązek przygotowania zgłoszenia zbiorów danych osobowych podlegających rejestracji oraz obowiązek ich aktualizacji ciąży na ABI.

§5.1. W razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, Administrator jest obowiązany, bez zbędnej zwłoki, do uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru.

2. Administrator jest obowiązany poinformować bez zbędnej zwłoki innych administratorów, którym udostępnił zbiór danych, o dokonanym uaktualnieniu lub sprostowaniu danych.

ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI I ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, ABI, ASI.
Do wiadomości: Osoby upoważnione.

§6.1.Administrator wyznacza odrębnym zarządzeniem i zgłasza do rejestru prowadzonego przez GIODO administratora bezpieczeństwa informacji, który jest odpowiedzialny za przetwarzanie danych zgodnie z ustawą oraz rozporządzeniem. Zgłoszenie, o którym mowa dokonuje się według wzoru określonego rozporządzeniem Ministra Administracji i Cyfryzacji.

2.Zgodnie z przyjętą polityką delegowania uprawnień i zastępowalności Administrator wyznacza zastępcę ABI, który wykonuje wszystkie obowiązki należące do zakresu obowiązków ABI podczas jego nieobecności. Funkcję tę pełni ASI, wyznaczony odrębnym zarządzeniem. Zastępca ABI spełnia wszystkie warunki ustawowe, jak dla powołania ABI.

3. W celu skutecznego nadzorowania i ochrony przetwarzania danych Starosta Łowicki zobowiązuje kierowników do współdziałania z ABI, wpisując stosowne zakresy czynności i odpowiedzialności za nadzór nad przestrzeganiem przez podległych pracowników zapisów polityki bezpieczeństwa stosowanej w Starostwie Powiatowym w Łowiczu.

§7.1. Do zadań ABI należy:

1) **zapewnianie przestrzegania przepisów** o ochronie danych osobowych, w szczególności przez:
   a) **sprawdzanie zgodności przetwarzania danych osobowych** z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla Administratora,
   b) **nadzorowanie** opracowania i aktualizowania dokumentacji, ochrony danych osobowych oraz przestrzegania zasad w niej określonych,
   c) **zapewnianie zapoznania osób upoważnionych** do przetwarzania danych osobowych z przepisami o ochronie danych osobowych („szkolenie");
2) **prowadzenie rejestru zbiorów danych** przetwarzanych przez Administratora, z wyjątkiem zbiorów, wskazanych w ustawie jako zwolnione z obowiązku rejestracji, zawierającego w szczególności nazwę zbioru oraz spełniającego inne kryteria prawem przewidziane.

2. W celu sprawnej realizacji nałożonych zadań, ABI przysługują uprawnienia określone w rozporządzeniu Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. z 2015, poz. 745).

§8.1. Administratorem bezpieczeństwa informacji może być osoba, która spełnia warunki określone przepisami i zostanie zgłoszona do GIODO w terminie 30 dni od powołania.

2. Zarządzenie o którym mowa w §6 ust.1 wskazuje pracownika wymieniając z imienia i nazwiska osobę pełniącą tę funkcję.

3. Administrator danych może powierzyć ABI wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania przez ABI obowiązków.

4. Administrator bezpieczeństwa informacji podlega Staroście Łowickiemu;

5. Administrator zapewnia środki i organizacyjną odrębność ABI niezbędne do niezależnego wykonywania przez niego zadań.

§9.1. Administrator odrębnym zarządzeniem wyznacza Administratora Systemów Informatycznych, wymieniając z imienia i nazwiska osobę pełniącą tę funkcję.

2. ASI odpowiada za zapewnienie przestrzegania zasad ochrony danych osobowych przetwarzanych za pomocą systemów informatycznych określonych w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

3. Administrator wyznacza zastępcę ASI, zgodnie z przyjętą polityką delegowania uprawnień i zastępowalności. Zastępca ASI wykonuje wszystkie obowiązki należące do zakresu obowiązków ASI podczas jego nieobecności.

4. ASI podczas wykonywania obowiązków z zakresu ochrony danych osobowych podlega Administratorowi.

5. W przypadku niewyznaczenia ASI za zapewnienie przestrzegania zasad ochrony danych osobowych przetwarzanych za pomocą systemów informatycznych odpowiada Administrator.

PRZETWARZANIE DANYCH

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, ABI, ASI, osoby upoważnione.

§10.1. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:

1) **osoba, której dane dotyczą wyrazi na to zgodę**, chyba że chodzi o usunięcie dotyczących jej danych;

2) **jest to niezbędne dla zrealizowania uprawnienia** lub spełnienia obowiązku wynikającego z przepisu prawa;

3) **jest to konieczne do realizacji umowy**, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą;

4) **jest niezbędne** do wykonania określonych prawem zadań realizowanych dla dobra publicznego;

5) **jest to niezbędne** dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez Administratora albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

2. Za prawnie uzasadniony cel Administratora uznaje się w szczególności dochodzenie roszczeń z tytułu prowadzonej działalności, realizacji zadań nałożonych na jednostkę.

§11.1. Zgoda na przetwarzanie danych osobowych, nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

2. Zgoda na przetwarzanie danych osobowych może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania.

3. Zgoda na przetwarzanie danych osobowych może zostać odwołana w każdym czasie. W przypadku odwołania zgody na przetwarzanie danych osobowych Administrator obowiązany jest

usunąć wszystkie dane osobowe osoby, która zgodę cofnęła, chyba że istnieje inna podstawa prawna upoważniająca Administratora do dalszego przetwarzania tych danych dla innych celów niż wskazany w cofniętej zgodzie. Zaleca się odbieranie zgody w postaci możliwej do późniejszego uwodnienia.

§12.1. W przypadku powzięcia jakichkolwiek wątpliwości, co do ewentualnej zgodności z prawem planowanych działań w zakresie przetwarzania danych, należy zwrócić się do ABI z wnioskiem (ustnym/pisemnym) o ich rozstrzygnięcie.

2. Przed udzieleniem przez ABI odpowiedzi w przedmiocie istniejących wątpliwości niedozwolone jest zbieranie danych osobowych i ich utrwalanie, a w przypadku posiadania już danych osobowych których wątpliwość dotycz należy, do czasu rozstrzygnięcia wątpliwości, wstrzymać wszystkie działania na danych osobowych, co do których istnieją wątpliwości czy są prawnie uzasadnione.

POWIERZENIE PRZETWARZANIA DANYCH

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, ABI, ASI.
Do wiadomości: Osoby upoważnione.

§13.1Administrator może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.

2.Podmiot, któremu dane do przetwarzania powierzono, może przetwarzać dane wyłącznie w zakresie i w celu przewidzianym w umowie.

3. Zapisy z wzoru umowy powierzenia mogą być użyte do zmodyfikowania każdej umowy zawieranej z podmiotem, gdy jej prawidłowe wykonanie będzie wiązać się z koniecznością powierzenia przetwarzania danych osobowych.
Wzór umowy powierzenia stanowi załącznik nr1 ***Umowa powierzenia*** do polityki bezpieczeństwa.

3.Podmiot, któremu powierzono przetwarzanie danych obowiązany jest przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające przetwarzanie danych, o których mowa w ustawie oraz w rozporządzeniu.

4. Kierownik, po podpisaniu umowy, o której mowa w ust.1, przekazuje niezwłocznie informację do ABI, według wzoru stanowiącego załącznik nr 1a ***Ewidencja umów powierzenia*** do polityki bezpieczeństwa.

WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, ABI, ASI.
Do wiadomości: Osoby upoważnione.

§14.1. Administrator prowadzi wykaz zbiorów danych osobowych, które posiada.

2. Przy opisie każdego ze zbiorów wskazuje się programy zastosowane do przetwarzania danych.

3. Zbiory danych osobowych posiadane przez Administratora wraz z programami zastosowanymi do przetwarzania zawartych w nich danych wymienione zostały w załączniku nr 2 ***Wykazy - obszary, zbiory i przepływy*** do polityki bezpieczeństwa.

OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I POWIĄZANIA POMIĘDZY NIMI

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, ABI, ASI.
Do wiadomości: Osoby upoważnione.

§15. Struktura zbiorów danych osobowych wraz ze wskazaniem poszczególnych pól informacyjnych i powiązania pomiędzy nimi wskazane zostały załączniku nr 2 ***Wykazy - obszary, zbiory i przepływy*** do polityki bezpieczeństwa.

SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, ABI, ASI.
Do wiadomości: Osoby upoważnione.

§16. Sposób przepływu danych pomiędzy poszczególnymi systemami wskazany został w załączniku nr 2 ***Wykazy - obszary, zbiory i przepływy*** do polityki bezpieczeństwa.

PLAN SPRAWDZEŃ ORAZ DOKONYWANIE SPRAWDZEŃ

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, ABI, ASI.
Do wiadomości: Osoby upoważnione.

§17.1. Administrator bezpieczeństwa informacji celem zapewnienia zgodnego z prawem przetwarzania danych osobowych dokonuje sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowuje sprawozdanie w tym zakresie.

2. Sprawdzenie jest dokonywane dla Administratora lub Generalnego Inspektora. Sprawdzenie może być doraźne, planowe lub na żądanie Generalnego Inspektora.

§18.1. ABI zawiadamia Administratora o rozpoczęciu sprawdzenia doraźnego lub sprawdzenia na żądanie Generalnego Inspektora przed podjęciem pierwszej czynności.

2. Administrator bezpieczeństwa informacji zawiadamia kierownika, osobę zatrudnioną na samodzielnym stanowisku o zakresie planowanych czynności w terminie co najmniej 7 dni przed dniem przeprowadzenia czynności.

3. Zawiadomienia nie przekazuje się w przypadku:

1) sprawdzenia doraźnego, jeżeli niezwłoczne rozpoczęcie sprawdzenia jest niezbędne do przywrócenia stanu zgodnego z prawem lub weryfikacji, czy naruszenie miało miejsce;

2) sprawdzenia, o którego dokonanie zwrócił się Generalny Inspektor, jeżeli na zawiadomienie nie pozwala wyznaczony przez niego termin;

3) jeżeli kierownik komórki organizacyjnej Starostwa objętej sprawdzeniem posiada informacje, o zakresie planowanych czynności.

§18.1. ABI przygotowuje plan sprawdzeń.

2. Plan sprawdzeń zawiera przedmiot, zakres, termin sprawdzeń oraz sposób i zakres ich dokumentowania.

3. Plan sprawdzeń przygotowywany jest na okres nie krótszy niż kwartał i nie dłuższy niż rok. Plan sprawdzeń jest przedstawiany Staroście Łowickiemu nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem. Plan sprawdzeń obejmuje co najmniej jedno sprawdzenie.

4. Zbiory danych oraz systemy informatyczne służące do przetwarzania lub zabezpieczania danych osobowych podlegają sprawdzeniu nie rzadziej niż raz na pięć lat.

§19.1. Po zakończeniu sprawdzenia ABI przygotowuje sprawozdanie.

2. Sprawozdanie jest sporządzane w wersji papierowej i przekazywane do Administratora.

3. Administrator bezpieczeństwa informacji przekazuje Administratorowi sprawozdanie:

1) **ze sprawdzenia planowego** - nie później niż w terminie 30 dni od zakończenia sprawdzenia;

2) **ze sprawdzenia doraźnego** - niezwłocznie po zakończeniu sprawdzenia;

3) **ze sprawdzenia, o którego dokonanie zwrócił się Generalny Inspektor** - zachowując termin wskazany przez Generalnego Inspektora.

REJESTR ZBIORÓW DANYCH OSOBOWYCH PROWADZONY PRZEZ ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, ABI, ASI.
Do wiadomości: Osoby upoważnione.

§20.1. ABI prowadzi rejestr zbiorów danych osobowych w wersji papierowej lub elektronicznej, z możliwością jego wydruku.

2. W rejestrze nie ujawnia się zbiorów danych osobowych podlegających wyłączeniu od obowiązku rejestracji, zgodnie z art. 43 ustawy.

3. Rejestr jest jawny i każdy ma prawo do jego przeglądania. Udostępnianie rejestru następuje w formie wydruku, w siedzibie Starostwa Powiatowego w Łowiczu ul. Stanisławskiego 30, osobą wyznaczoną do udostępnienia rejestru jest ABI.

Wzór rejestru stanowi załącznik nr 3 ***Rejestr zbiorów danych osobowych*** do niniejszej polityki bezpieczeństwa.

OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, ABI, ASI.
Do wiadomości: Osoby upoważnione.

§21.1. Administrator, na pisemny wniosek kierownika, nadaje upoważnienie do przetwarzania danych osobowych każdej osobie, która do przetwarzania danych będzie dopuszczona. Wydanie upoważnienia jest związane z podpisaniem przez upoważnionego stosownego oświadczenia, potwierdzającego znajomość przepisów w tym zakresie.
Wzór wniosku, stanowi załącznik nr 4 ***Wniosek o nadanie uprawnień*** do polityki bezpieczeństwa.

2. Upoważnienie zawiera:

1) datę z którą zostało nadane, znak sprawy(z rejestru upoważnień);

2) datę z którą upoważnienie wygasa jeżeli jest ono nadane na czas określony;

3) zakres upoważnienia.

3. Upoważnienie do przetwarzania danych osobowych wygasa z chwilą upływu terminu wypowiedzenia lub rozwiązania umowy zawartej przez Administratora z osobą, której zostało nadane lub w przypadku gdy zostało nadane na czas określony z upływem czasu na jaki zostało nadane.

4. Zmiana stanowiska lub/i inny zakres obowiązków jest związany z koniecznością złożenia przez kierownika wniosku do Administratora o nadanie nowego upoważnienia i cofnięcia poprzednich.

5. Na podstawie złożonego wniosku, o którym mowa w ust.1, po zaakceptowaniu przez ABI są przygotowywane dokumenty. Wniosek można przekazać w wersji papierowej lub elektronicznie na adres e-mail ABI.

6. Upoważnienie wraz z oświadczeniem jest przygotowywane w trzech egzemplarzach. Podpisane przez Administratora upoważnienie ABI przekazuje kierownikowi. Pracownik po zapoznaniu się z przepisami z zakresu ochrony danych osobowych i odbytym szkoleniu, o którym mowa w §23 potwierdza, składając podpis, znajomość przepisów w tym zakresie.
Kierownik przekazuje podpisane trzy egzemplarze, jeden pracownikowi, dwa wydziałowi organizacyjnemu oraz niezwłocznie drogą elektroniczną informuje ABI o tym fakcie, podając datę przyjęcia upoważnienia przez osobę upoważnioną.
Wzór upoważnienia stanowi załącznik nr 5 ***Upoważnienie do przetwarzania danych osobowych,*** natomiast wzór oświadczenia stanowi załącznik nr 6 ***Oświadczenie*** do polityki bezpieczeństwa.

7. Odpowiedzialność służbową za przetwarzanie danych osobowych tylko przez osoby, które przeszły szkolenie i są upoważnione przez Administratora danych osobowych, ponosi kierownik. Skierowanie na szkolenie, termin kierownik ustala wysyłając zgłoszenie pocztą elektroniczną do ABI.

8. Osoba upoważniona przez Administratora nie ma prawa do nadawania dalszych upoważnień, chyba że upoważnienie do przetwarzania danych osobowych nadane przez Administratora zawiera upoważnienie do nadawania dalszych upoważnień.

9. Każdy kto przetwarza dane osobowe obowiązany jest zachować w tajemnicy dane osobowe do których posiada dostęp zarówno zamierzony jak i przypadkowy, sposoby zabezpieczania danych jak również wszelkie informacje, które powzięły w czasie przetwarzania danych. Obowiązek zachowania danych w tajemnicy jest bezterminowy.

10. Zachowanie tajemnicy w zakresie danych osobowych dotyczy również wszystkich osób wykonujących zadania na rzecz Starostwa oraz pełniących funkcję w administracji budynków do których mają dostęp, zarówno zamierzony jak i przypadkowy, do wszelkich informacji, które powzięły w czasie pracy w Starostwie Powiatowym w Łowiczu. Obowiązek zachowania danych w tajemnicy jest bezterminowy, udokumentowany podpisanym oświadczeniem, które jest załączone do akt osobowych/ umowy. Wzór oświadczenia stanowi załącznik nr 6a ***Oświadczenie*** do polityki bezpieczeństwa.

11. Podczas przetwarzania danych należy zachować szczególną ostrożność i podjąć wszelkie możliwe środki umożliwiające zabezpieczenie oraz ochronę danych przed nieuprawnionym dostępem, modyfikacją, zniszczeniem lub ujawnieniem.

12. Należy dochować należytej staranności podczas przesyłania dokumentów zawierających dane za pomocą środków komunikacji elektronicznej, w szczególności należy upewnić się, czy przesyłane za pomocą poczty elektronicznej dokumenty trafiły do właściwego odbiorcy.

13. Wszyscy pracownicy są zobowiązani do bezwzględnego umieszczenia w swoich e-mailach służbowych informacji identyfikującej pracownika wraz z podaniem stanowiska, wydziału/ biura, telefonu służbowego oraz umieszczenia w stopce informacji (wg. wzoru):

w podpisie

Aneta Kowalska
Inspektor w Wydziale Komunikacji
Starostwo Powiatowe w Łowiczu
ul. Stanisławskiego 28, 99-400 Łowicz
Tel:
e-mail;
w stopce

Powiat Łowicki 99-40 Łowicz ul. Stanisławskiego 30
tel.: +48 46 837-59-02; fax. +48 46 837 50 15; NIP: 834-18-82-519; Regon: 750 14 77 68,
Treść tej wiadomości, wraz z ewentualnymi załącznikami, zawiera informacje przeznaczone tylko dla wymienionego w niej adresata i może zawierać informacje, które są poufne oraz prawnie chronione. Jeżeli nie są Państwo jej adresatem, bądź otrzymali ją przez pomyłkę należy: powiadomić niezwłocznie nadawcę poprzez odesłanie zwrotnej odpowiedzi na tą wiadomość, usunąć wiadomość w całości, nie ujawniać, nie rozpowszechniać, nie powielać i nie używać jej w jakikolwiek sposób w całości lub w części w jakiejkolwiek formie.

14. W przypadku przesyłania za pomocą środków komunikacji elektronicznej zestawień, spisów czy innych dokumentów zawierających dane osobowe, przesyłany dokument należy zaszyfrować, a hasło przesłać w miarę możliwości innym środkiem komunikacji elektronicznej.

EWIDENCJA OSÓB UPOWAŻNIONYCH

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, ABI, ASI.
Do wiadomości: Osoby upoważnione.

§22.1 Administrator prowadzi ewidencję osób upoważnionych, ewidencja jest prowadzona w wersji elektronicznej z możliwością jej wydruku.

2. Ewidencja zawiera:

1) imię i nazwisko osoby upoważnionej;
2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych;
3) Identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

Wzór ewidencji stanowi załącznik nr 7 ***Ewidencja osób upoważnionych*** do polityki bezpieczeństwa.

SZKOLENIA

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, ABI, ASI.
Do wiadomości: Osoby upoważnione.

§23.1. Szkolenie dla osób, które mają otrzymać upoważnienie w zakresie obowiązujących przepisów, procedur oraz podstawowych zagrożeń związanych z przetwarzaniem danych jest prowadzone przez ABI/inne podmioty. W szkoleniu uczestniczą również osoby, od których należy odebrać oświadczenie o którym mowa w §21 ust.10.

2. Szkolenie **wstępne** jest przeprowadzane przed dopuszczeniem osoby upoważnionej do czynności przetwarzania danych, przed nadaniem upoważnienia lub odebrania oświadczenia o zachowaniu tajemnicy.

3. Szkolenia **cykliczne**, minimum raz w roku dla wszystkich pracowników oraz zarządu prowadzi ABI lub/i ASI. Z przeprowadzonego szkolenia jest sporządzana lista obecności. Wiedza z zakresu ochrony danych osobowych jest systematycznie sprawdzana. ABI informuje kierowników o terminach i formie sprawdzenia wiedzy. Wyniki są przekazywane w formie pisemnej do Administratora, celem podjęcia stosownych działań.

WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ TWORZĄCYCH OBSZAR W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, ABI, ASI.
Do wiadomości: Osoby upoważnione.

§24.1. Administrator przetwarza dane jedynie w pomieszczeniach do tego przeznaczonych w sposób uniemożliwiający dostęp do danych osobom nieuprawnionym.

2. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar w którym przetwarzane są dane osobowe zawarty został w załączniku nr 2 ***Wykazy - obszary, zbiory i przepływy*** do polityki bezpieczeństwa.

OKREŚLENIE ŚRODKÓW TECHNICZNYCH ORGANIZACYJNYCH NIEZBĘDNNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, ABI, ASI, osoby upoważnione.
Do wiadomości: Osoby upoważnione.

§25.1. Każdy kto przetwarza dane osobowe obowiązany jest zachować w tajemnicy dane osobowe do których posiada dostęp zarówno zamierzony jak i przypadkowy, sposoby zabezpieczania danych jak również wszelkie informacje, które powziął w czasie przetwarzania danych. Obowiązek zachowania danych w tajemnicy jest bezterminowy.

2. Podczas przetwarzania danych należy zachować szczególną ostrożność i podjąć wszelkie możliwe środki umożliwiające zabezpieczenie oraz ochronę danych przed nieuprawnionym dostępem, modyfikacją, zniszczeniem lub ujawnieniem.

3. Hasła i loginy do systemu informatycznego nie mogą być ujawniane nawet po utracie ich ważności.

4. Należy dochować należytej staranności podczas przesyłania dokumentów zawierających dane za pomocą środków komunikacji elektronicznej, w szczególności należy upewnić się czy przesyłane za pomocą poczty elektronicznej dokumenty trafiły do właściwego odbiorcy.

5. W przypadku przesyłania za pomocą środków komunikacji elektronicznej zestawień, spisów czy innych dokumentów zawierających dane osobowe, przesyłany dokument należy zaszyfrować, a hasło przesłać, w miarę możliwości innym środkiem komunikacji elektronicznej.

§26.1.Wszelkie dokumenty zwierające dane osobowe przechowywane są w szafach lub pomieszczeniach zamykanych na klucz.

2. Osoba będąca dysponentem kluczy jest zobowiązana nie przekazywać kluczy do budynków i pomieszczeń w których przetwarzane są dane osobom nieuprawnionym, a ponadto obowiązana jest przedsięwziąć działania celem wykluczenia ryzyka ich utraty.

3.Osoba która utraciła posiadane klucze do pomieszczeń Administratora w których przetwarzane są dane, niezwłocznie zgłasza tę okoliczność ABI, Administratorowi.

4. ABI lub Administrator podejmują wszelkie niezbędne środki techniczne i organizacyjne w celu zabezpieczenia pomieszczenia, do którego klucze utracono.

5. W Starostwie Powiatowym w Łowiczu, zgodnie z zasadami organizacji pracy wydanymi przez Sekretarza Powiatu Łowickiego, w imieniu Administratora, klucze (3 komplety) do pomieszczeń są wydawane i odbierane przez upoważnione osoby. Klucze (jeden komplet znajduje się w gablocie) są pobierane przed rozpoczęciem pracy i zdawane po jej zakończeniu. Czynność ta jest odnotowana w książce pobranych kluczy. Dwa komplety - zapasowy/ awaryjny znajduje się u dysponenta kluczy zapasowych i jest wydawany tylko w sytuacji awaryjnej. W przypadku wystąpienia sytuacji zagrożenia dyżurny, który jest pracownikiem biura ZK pobiera klucze z gabloty, fakt pobrania jest odnotowany w książce pobranych kluczy. Każde użycie klucza w przypadku awarii/zagrożenia wiąże się z koniecznością poinformowania Administratora i ABI.

7. Pomieszczenia, które są szczególnie istotne ze względu bezpieczeństwa informacji posiadają dodatkowe zabezpieczenia w postaci kodów dostępu oraz kart elektronicznych. Dostęp do tych pomieszczeń mają tylko osoby upoważnione. **Rejestr osób upoważnionych** jest prowadzony przez ASI/ osobę wyznaczoną.

8.Szczegółowy wykaz środków technicznych i organizacyjnych stosowanych przez Administratora celem zapewnienia poufności, integralności i rozliczalności przetwarzanych danych zawarty został w załączniku nr 2 ***Wykazy - obszary, zbiory i przepływy*** do polityki bezpieczeństwa.

§27.1. Osoba przetwarzająca dane po zakończeniu pracy porządkuje swoje stanowisko zabezpieczając dokumenty i nośniki elektroniczne z danymi w specjalnie do tego przeznaczonych szafach lub pomieszczeniach.

2.Niszczenie dokumentów zawierających dane odbywa się jedynie za pomocą niszczarki gwarantującej odpowiedni stopień rozdrobnienia (zaleca się, aby niszczarka spełniała wymogi normy DIN 66399, klasa bezpieczeństwa nie niższa niż 3) lub za pośrednictwem firmy zajmującej się niszczeniem dokumentów.

3.Każdy dokument zawierający dane, a nieużyteczny niszczy się niezwłocznie.

4.Podczas korzystania z urządzeń wielofunkcyjnych należy zachować szczególną ostrożność. Dokumenty kopiowane bądź skanowane wyjmowane są z urządzenia wielofunkcyjnego niezwłocznie po ich użyciu. Dotyczy to również dokumentów powstałych na skutek kopiowania bądź skanowania.

5.Przebywanie osób trzecich w obszarze, w którym przetwarzane są dane jest dopuszczalne za zgodą Administratora lub w obecności osoby upoważnionej.

6.Szczegółowy opis środków bezpieczeństwa zastosowanych przez Administratora wskazany został w załączniku nr 2 ***Wykazy - obszary, zbiory i przepływy*** do polityki bezpieczeństwa.

POSTĘPOWANIE W RAZIE ZAISTNIENIA ZAGROŻENIA DLA BEZPIECZEŃSTWA PRZETWARZANYCH DANYCH OSOBOWYCH LUB NARUSZENIA ZASAD PRZETWARZANIA DANYCH OSOBOWYCH

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, ABI, ASI, osoby upoważnione.

§28.1. W przypadku podejrzenia naruszenia zasad bezpieczeństwa danych osobowych lub naruszenia zabezpieczeń stosowanych przez Administratora dla ochrony przetwarzanych danych osobowych należy niezwłocznie zawiadomić ABI, w razie jego nieobecności ASI o dostrzeżonych lub podejrzewanych naruszeniach. Zgłoszenie może zostać przekazywane telefonicznie lub elektronicznie, na adres e-mail ABI/ASI.

2.W przypadku opisanym w ust. 1 ABI/ ASI przeprowadza sprawdzenie doraźne. Sprawdzenie jest dokonywane niezwłocznie.

3.Przy dokonywaniu sprawdzenia ABI/ASI przysługują uprawnienia wskazane w rozporządzeniu ministra administracji i cyfryzacji w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji, a w szczególności prawo:

1) utrwalenia danych z systemu informatycznego służącego do przetwarzania lub zabezpieczania na informatycznym nośniku danych lub dokonania wydruku tych danych;
2) odebrania wyjaśnień osoby, której czynności objęto sprawdzeniem;
3) sporządzeniu kopii otrzymanego dokumentu;
4) sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych.

4.Wykaz przykładowych sytuacji stanowiących naruszenie przyjętych zasad bezpieczeństwa stanowi załącznik nr 8 ***Przykładowe incydenty ODO*** do polityki bezpieczeństwa.

5. ABI/ASI dokonuje rejestracji naruszeń, których mowa w ust.1 w rejestrze incydentów, wzór określa załącznik nr 9 ***Rejestr incydentów*** do polityki bezpieczeństwa.

POSTANOWIENIA KOŃCOWE

§29.1. Dokumentacja przetwarzania danych osobowych stanowi wewnętrzną regulację Starosty Łowickiego, jako Administratora i obowiązuje wszystkich pracowników i współpracowników Starostwa.

2. Dokumentacja przetwarzania danych osobowych obowiązuje od dnia jej wprowadzenia w życie, zgodnie z zarządzeniem Starosty Łowickiego. Wszelkie zmiany dokumentacji przetwarzania danych osobowych obowiązują od dnia ich wprowadzenia w życie, zgodnie z zarządzeniem zmieniającym.

3. Każdy kto przetwarza dane posiadane przez Administratora zobowiązany jest do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej dokumentacji przetwarzania danych osobowych

4. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.

5. W sprawach nieuregulowanych w niniejszej polityce bezpieczeństwa mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy ustaw.

STAROSTA ŁOWICKI

Krzysztof Figat

Wzór - możliwa modyfikacja

Załącznik nr 1
do Polityki bezpieczeństwa przetwarzania danych osobowych w Starostwie Powiatowym w Łowiczu wprowadzonej
Zarządzeniem Nr ..17/2016
Starosty Łowickiego z dnia 21 marca 2016r.

Umowa powierzenia przetwarzania danych osobowych

zawarta w Łowiczu dnia .....pomiędzy:

Starostą Łowickim z siedzibą w Łowiczu, ul. Stanisławskiego 30, 99-400 Łowicz

zwanym w dalszej części umowy „*Zleceniodawcą*"

oraz
(*dane podmiotu który umowę zawiera, w szczególności: firma spółki, siedziba, adres, oznaczenie sądu rejestrowego, w którym przechowywana jest dokumentacja spółki oraz numer pod którym spółka jest wpisana do rejestru; NIP, wysokość kapitału zakładowego i kapitału wpłaconego – art. 206 lub 374 ksh. W przypadku podmiotów prowadzących działalność gospodarczą imię nazwisko adres zamieszkania osoby fizyczne, PESEL, firma pod jaką działalność jest prowadzona oraz adres głównego miejsca wykonywania działalności*).

zwanym w dalszej części umowy „Zleceniobiorcą"
reprezentowanym przez:

……

Powierzenie przetwarzania danych osobowych

§1.1. Zleceniodawca powierza Zleceniobiorcy, w trybie art. 31 ustawy z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych* (Dz.U. z 2015 r. poz. 2135 „*Ustawą*") dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.

2. Zleceniodawca oświadcza, że Administratorem danych, które powierza Zleceniobiorcy do przetwarzania jest Starosta Łowicki z siedzibą w Łowiczu, ul. Stanisławskiego 30; 99-400 Łowicz.

4. Zleceniodawca powierza Zleceniobiorcy przetwarzanie danych osobowych w zakresie określonym w niniejszej umowie.

Zakres i cel przetwarzania danych

§2.1. Zleceniobiorca będzie przetwarzał, powierzone na podstawie umowy, następujące dane osobowe:

1) imiona, nazwisko;
2) adres zamieszkania lub zameldowania;
4) numer telefonu*

2. Powierzone przez Zleceniodawcę dane osobowe będą przetwarzane przez Zleceniobiorcę wyłącznie w celu*

.....,

w sposób zgodny z treścią umowy i jedynie przez czas jej trwania.

Sposób wykonania umowy w zakresie przetwarzania danych osobowych

§3.1. Zleceniobiorca zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez podjęcie środków technicznych i organizacyjnych, o których mowa w szczególności w art. 36 – 39 a Ustawy.

2. Zleceniobiorca oświadcza, że zgodnie z rozporządzeniem 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 informacyjne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024):

1) prowadzi dokumentację opisującą sposób przetwarzania danych osobowych;

2) znajdujące się w jego posiadaniu urządzenia i systemy informatyczne służące do przetwarzania danych osobowych zapewniają poziom bezpieczeństwa określony jako wysoki;

3) stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności zabezpiecza dane osobowe przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy, zmianą, utratą, uszkodzeniem lub zniszczeniem.

3. Zleceniobiorca zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, Ustawą oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.

4. Zleceniobiorca może powierzyć dane osobowe objęte niniejszą Umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Zleceniodawcy.

Odpowiedzialność Zleceniobiorcy

§4. Zleceniobiorca jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.

Czas obowiązywania umowy

§5.1. Niniejsza umowa zostaje zawarta na czas nieokreślony/ określony do dnia** .

2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem..... okresu wypowiedzenia***.

3. Zleceniodawca ma prawo rozwiązać umowę w trybie natychmiastowym, gdy Zleceniobiorca:

1) wykorzystuje dane osobowe w sposób niezgodny z umową, na co Zleceniodawca zwróci Zleceniobiorcy uwagę na piśmie, a Zleceniobiorca w wyznaczonym przez Zleceniodawcę terminie nie usunie wskazanych naruszeń;

2) nie zaprzestanie niewłaściwego przetwarzania danych osobowych, na co Zleceniodawca zwróci Zleceniobiorcy uwagę na piśmie, a Zleceniobiorca w wyznaczonym przez Zleceniodawcę terminie nie usunie wskazanych naruszeń;

Zasady zachowania poufności

§6.1. Zleceniobiorca zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Zleceniodawcy i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne").

2. Zleceniobiorca oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Zleceniodawcy innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

3. Strony zobowiązują się do dołożenia wszelkich starań w celu zapewnienia, aby środki łączności wykorzystywane do odbioru, przekazywania oraz przechowywania danych poufnych gwarantowały zabezpieczenie danych poufnych w tym w szczególności danych osobowych powierzonych do przetwarzania, przed dostępem osób trzecich nieupoważnionych do zapoznania się z ich treścią.

§7. Zmiana niniejszej Umowy może nastąpić tylko w formie pisemnego aneksu.

§8.W sprawach nieuregulowanych niniejszą Umową mają zastosowania przepisy z ustawy o.d.o. oraz ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. D.z U. z 2014 r. poz. 121 z późn. zm.)

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

.....	.....
Zleceniodawca	Zleceniobiorca

* *należy uzupełnić odpowiednio, w zależności od tego jakie dane zostaną powierzone i jaki jest cel powierzenia przetwarzania danych.*
** *wpisujemy datę obowiązywania umowy*
*** *dotyczy umowy na czas nieokreślony*

STAROSTA ŁOWICKI
Krzysztof Figat

wzór

Załącznik nr 1a
do Polityki bezpieczeństwa przetwarzania danych osobowych
w Starostwie Powiatowym w Łowiczu
wprowadzonej Zarządzeniem Nr 17/2016
Starosty Łowickiego z dnia 21 marca 2016r.

EWIDENCJA UMÓW POWIERZENIA

L.p./ Data	Nazwa podmiotu / siedziba/osoba do kontaktu ADO/ABI	Data podpisania	Data zakończenia	Nr umowy / zakres przetwarzania danych osobowych (nazwa zbioru, cel przetwarzania)	Wydział/ biuro	Kierownik wydziału/biura zgłaszający umowę powierzenia do ABI
1						
2						
3						
4						
5						

STAROSTA ŁOWICKI

Krzysztof Figat

Wzór

Załącznik nr 2
do Polityki bezpieczeństwa przetwarzania danych osobowych
w Starostwie Powiatowym w Łowiczu
wprowadzonej Zarządzeniem Nr 17/2016
Starosty Łowickiego z dnia 21 marca 2016 r.

WYKAZY- obszary, zbiory i przepływy

A. WYKAZ BUDYNKÓW POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ TWORZĄCYCH OBSZAR W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE WRAZ Z OKREŚLENIEM ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

[dane Administratora]		
WYKAZ BUDYNKÓW	**POŁOŻENIE (ADRES)**	**STOSOWANE ŚRODKI TECHNICZNE I ORGANIZACYJNE**
SIEDZIBA	[adres siedziby]	monitoring/alarm/ochrona całodobowa/system kontroli dostępu/gaśnice/szafy zamykane na klucz/szafy metalowe/rolety antywłamaniowe/ewidencja osób wchodzących i wychodzących/ewidencja kierowców.
ODDZIAŁ ZAMIEJSCOWY	[adres oddziałów zamiejscowych]	monitoring/alarm/ochrona całodobowa/system kontroli dostępu/gaśnice/szafy zamykane na klucz/szafy metalowe/rolety antywłamaniowe/ewidencja osób wchodzących i wychodzących/ewidencja kierowców.
ARCHIWUM	[adres archiwum]	monitoring/alarm/ochrona całodobowa/system kontroli dostępu/gaśnice/szafy zamykane na klucz/szafy metalowe/rolety antywłamaniowe/ewidencja osób wchodzących i wychodzących/ewidencja kierowców.
MAGAZYN	[adresy magazynów]	monitoring/alarm/ochrona całodobowa/system kontroli dostępu/gaśnice/szafy zamykane na klucz/szafy metalowe/rolety antywłamaniowe/ewidencja osób wchodzących i wychodzących/ewidencja kierowców.
MIEJSCE PRZECHOWYWANIA KOPII BEZPIECZEŃSTWA	[miejsce przechowywania kopii bezpieczeństwa]	monitoring/alarm/ochrona całodobowa/system kontroli dostępu/gaśnice/szafy zamykane na klucz/szafy metalowe/rolety antywłamaniowe/ewidencja osób wchodzących i wychodzących/ewidencja kierowców.

B. WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH ORAZ OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I POWIĄZANIA POMIĘDZY NIMI

NAZWA ZBIORU DANYCH	PROGRAM ZASTOSOWANY DO PRZETWARZANIA DANYCH W ZBIORZE	OPIS STRUKTURY ZBIORÓW DANYCH – ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH	OPIS STRUKTURY ZBIORÓW DANYCH – POWIĄZANIA POMIĘDZY ZBIORAMI

C. SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

SYSTEM Z KTÓREGO DANE WYPŁYWAJĄ	SYSTEM DO KTÓREGO NASTEPUJE PRZEPŁYW DANYCH	UWAGI

STAROSTA ŁOWICKI

Krzysztof Figat

wzór

Załącznik nr 3
do Polityki bezpieczeństwa przetwarzania danych osobowych
w Starostwie Powiatowym w Łowiczu
wprowadzonej Zarządzeniem Nr 17/2016
Starosty Łowickiego z dnia 21 marca 2016 r.

Lp	REJESTR ZBIORU DANYCH	
	Numer wpisu	ZDO-000
1	Nazwa zbioru	
2	Administrator Danych, jego adres	
3	Oznaczenie przedstawiciela administratora danych zgodnie z art. 31a	
4	Oznaczenie przedstawiciela administratora danych zgodnie z art. 31	
5	Podstawa prawna upoważniająca do prowadzenia zbioru danych	
6	Cel przetwarzania danych w zbiorze	
7	Opis kategorii osób, których dane są przetwarzane w zbiorze	
8	Zakres danych przetwarzanych w zbiorze	
9	Sposób zbierania danych do zbioru	
10	Sposób udostępniania danych ze zbioru	
11	Oznaczenie odbiorców danych lub kategorii odbiorców	
12	Informacja dotycząca przekazania danych do państwa trzeciego	

Lp.	REJESTR ZBIORÓW DANYCH OSOBOWYCH				
	Nazwa zbioru danych osobowych	Data wpisania zbioru danych	Data ostatniej modyfikacji	Właściciel	Rejestr Zbioru Danych
1					
2					
3					
4					
5					
6					
7					
8					
9					

STAROSTA ŁOWICKI

Krzysztof Figat

Wzór- możliwa modyfikacja

Załącznik nr 4
do Polityki bezpieczeństwa przetwarzania danych osobowych w Starostwie Powiatowym w Łowiczu wprowadzonej Zarządzeniem Nr 17/2016
Starosty Łowickiego z dnia 21 marca 2016r.

Wniosek o nadanie uprawnień

☐ **dla użytkownika w systemie informatycznym**

☐ **upoważnienie do przetwarzania danych osobowych**

☐ **Nowy użytkownik**	☐ **Modyfikacja uprawnień**	☐ **Odebranie uprawnień- w systemie / do przetwarzania danych**

DOTYCZY SYSTEMU: .....

(nazwa aplikacji (bazy danych), w której przetwarzane są dane osobowe)

Imię i nazwisko użytkownika	**Komórka organizacyjna**	
Stanowisko	**Telefon nr**	
Posiada upoważnienie do przetwarzania danych osobowych:	☐ TAK	☐ NIE
Zakres uprawnień użytkownika w systemie informatycznym /dostęp do zbiorów danych osobowych, uzasadnienie *:		
Okres obowiązywania uprawnienia:		
Data zgłoszenia:	Podpis kierownika:	
ASI:	ABI:	

*należy napisać zakres: modyfikacja, odczyt, wprowadzenie, usuwanie, nazwa zbioru danych osobowych; w jakim zakresie dostęp do systemów informatycznych

STAROSTA ŁOWICKI
Krzysztof Figat

wzór --możliwa modyfikacja

Załącznik nr 5
do Polityki bezpieczeństwa przetwarzania danych osobowych w Starostwie Powiatowym w Łowiczu wprowadzonej Zarządzeniem Nr ...17/2016..... Starosty Łowickiego z dnia ..21 marca 2016 r.

.....
Znak sprawy

UPOWAŻNIENIE
do przetwarzania danych osobowych

Z dniem ..... upoważniam Panią/Pana.....

podać imię i nazwisko pracownika

do przetwarzania danych osobowych w następującym zakresie:

☐ dane przetwarzane w formie papierowej

☐ dane przetwarzane w systemie informatycznym

w tym dane osobowe objęte zbiorami:

1. „Nazwa zbioru A" w zakresie modyfikacja, odczyt, wprowadzenie i usuwanie danych
2. „Nazwa zbioru B" w zakresie odczyt

Niniejsze upoważnienie traci moc:
najpóźniej z dniem odwołania albo rozwiązania lub wygaśnięcia umowy o prace, umowy zlecenia, umowy o dzieło lub innej umowy cywilnoprawnej* łączącej Pana/Panią z Administratorem w tym również zmiana stanowiska pracy i związana z tym konieczność nadania innego upoważnienia.

Łowicz ,..... .....
data (Administrator Danych Osobowych)

- Niepotrzebne usunąć/wpisać datę – okres obowiązywania

Potwierdzam odbiór upoważnienia

Łowicz ....
Data Podpis pracownika

STAROSTA ŁOWICKI
Krzysztof Figat

Wzór- możliwa modyfikacja

Załącznik nr 6
do Polityki bezpieczeństwa przetwarzania danych osobowych w Starostwie Powiatowym w Łowiczu wprowadzonej Zarządzeniem Nr ....17/2016..... Starosty Łowickiego z dnia .21. marca .2016 r.

Łowicz, dnia ..... r.

.....
Imię i nazwisko

.....
Komórka organizacyjna

OŚWIADCZENIE

Oświadczam, iż zostałam/em zapoznana/y z przepisami dotyczącymi ochrony danych osobowych, w szczególności ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2015 poz. 2135), wydanych na jej podstawie aktów wykonawczych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Polityki Bezpieczeństwa oraz Instrukcji Zarządzania.

Zobowiązuję się do:

- zachowania w tajemnicy danych osobowych, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań służbowych lub obowiązków pracowniczych,
- niewykorzystywania danych osobowych w celach pozasłużbowych o ile nie są one jawne,
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych o ile nie są one jawne,
- korzystania ze sprzętu IT oraz oprogramowania wyłącznie w związku z wykonywaniem obowiązków,
- wykorzystywania jedynie legalnego oprogramowania pochodzącego od Administratora,
- należytej dbałości o sprzęt i oprogramowanie zgodnie z dokumentacją przetwarzania danych osobowych,
- korzystania z komputerów przenośnych zgodnie z dokumentacją przetwarzania danych osobowych,
- nieudostępniania sprzętu służbowego, w szczególności urządzeń mobilnych, osobom trzecim

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.

Łowicz .....
Data

.....
Podpis osoby upoważnionej

STAROSTA ŁOWICKI
Krzysztof Figat

Wzór- możliwa modyfikacja

Załącznik nr 6 a
do Polityki bezpieczeństwa przetwarzania
danych osobowych w Starostwie
Powiatowym w Łowiczu wprowadzonej
Zarządzeniem Nr ....17./2016.....
Starosty Łowickiego z dnia ..21 marca 2016 r.

Łowicz, dnia ..... r.

.....
Imię i nazwisko

.....
Komórka organizacyjna

OŚWIADCZENIE

Oświadczam, że zapoznałem/am się z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015r., poz. 2135).
Zobowiązuję się w okresie zatrudnienia w Starostwie Powiatowym w Łowiczu, jak również po ustaniu zatrudnienia do zachowania tajemnicy wszystkich danych osobowych do których będę miał/a dostęp w związku z wykonywaniem obowiązków służbowych.
Jestem świadomy/a odpowiedzialności karnej za udostępnianie lub umożliwienie dostępu do danych osobowych osobom nieupoważnionym.

Łowicz .....
Data

.....
Podpis

STAROSTA ŁOWICKI
Krzysztof Figat

Wzór

Załącznik nr 7
do Polityki bezpieczeństwa przetwarzania danych osobowych w Starostwie Powiatowym w Łowiczu wprowadzonej Zarządzeniem Nr ...17/2016.....
Starosty Łowickiego z dnia ...21 marca.

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Nazwisko i Imię osoby upoważnionej	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia do przetwarzania danych osobowych	Identyfikator (jeżeli dane przetwarzane są w systemie informatycznym)

Dane aktualne na dzień: .....

Podpis ADO: .....

STAROSTA ŁOWICKI

Krzysztof Figat

Załącznik nr 8
do Polityki bezpieczeństwa przetwarzania danych osobowych w Starostwie Powiatowym w Łowiczu wprowadzonej Zarządzeniem Nr 17/2016 Starosty Łowickiego z dnia 21 marca 2016r.

PRZYKŁADOWE INCYDENTY	
FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
W ZAKRESIE WIEDZY	
Ujawnianie sposobu działania aplikacji i systemu oraz jej zabezpieczeń osobom niepowołanym.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Bezzwłocznie powiadomić administratora bezpieczeństwa informacji (ABI).
Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej.	
Dopuszczanie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać np. z obserwacji lub dokumentacji.	
W ZAKRESIE SPRZĘTU I OPROGRAMOWANIA	
Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.	Niezwłocznie zakończyć działanie aplikacji. Bezzwłocznie powiadomić administratora bezpieczeństwa informacji (ABI).
Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony.	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Bezzwłocznie powiadomić administratora bezpieczeństwa informacji (ABI).
Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych lub sieci.	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Bezzwłocznie powiadomić administratora bezpieczeństwa informacji (ABI).
Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych osobom nieuprawnionym.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić, jakie czynności zostały przez osoby nieuprawnione wykonane. Przerwać działające programy. Bezzwłocznie powiadomić administratora bezpieczeństwa informacji (ABI).

Samodzielne instalowanie jakiegokolwiek oprogramowania.	Pouczyć osobę popełniającą wymienioną czynność, aby jej zaniechała. Wezwać służby informatyczne w celu odinstalowania programów. Bezzwłocznie powiadomić administratora bezpieczeństwa informacji (ABI).
Modyfikowanie parametrów systemu i aplikacji.	Wezwać osobę popełniającą wymieniona czynność, aby jej zaniechała. Bezzwłocznie powiadomić administratora bezpieczeństwa informacji (ABI).
W ZAKRESIE DOKUMENTÓW I OBRAZÓW ZAWIERAJĄCYCH DANE OSOBOWE	
Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru.	Zabezpieczyć dokumenty. Bezzwłocznie powiadomić administratora bezpieczeństwa informacji (ABI).
Przechowywanie dokumentów niewłaściwie zabezpieczonych przed dostępem osób niepowołanych.	Powiadomić przełożonych. Spowodować poprawienie zabezpieczeń. Bezzwłocznie powiadomić ABI.
Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Bezzwłocznie powiadomić administratora bezpieczeństwa informacji (ABI).
Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią.	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić przełożonych. Bezzwłocznie powiadomić administratora bezpieczeństwa informacji (ABI).
Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Jeżeli ujawnione zostały ważne dane - bezzwłocznie powiadomić administratora bezpieczeństwa informacji (ABI).
Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych procedurą.	Spowodować zaprzestanie kopiowania. Podjąć próbę odzyskania oraz zabezpieczyć wykonaną kopię. Bezzwłocznie powiadomić administratora bezpieczeństwa informacji (ABI).
Utrata kontroli nad kopią danych osobowych.	Podjąć próbę odzyskania kopii. Bezzwłocznie powiadomić administratora bezpieczeństwa informacji (ABI).

W ZAKRESIE POMIESZCZEŃ I INFRASTRUKTURY SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH	
Opuszczanie i pozostawianie bez dozoru nie zamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych.	Zabezpieczyć pomieszczenie. Powiadomić przełożonych. Bezzwłocznie powiadomić administratora bezpieczeństwa informacji (ABI).
Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym.	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość. Bezzwłocznie powiadomić administratora bezpieczeństwa informacji (ABI).
Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakiekolwiek urządzenia do sieci komputerowej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i ABI. Bezzwłocznie powiadomić administratora bezpieczeństwa informacji (ABI).
W ZAKRESIE POMIESZCZEŃ, W KTÓRYCH ZNAJDUJĄ SIĘ KOMPUTERY CENTRALNE I URZĄDZENIA SIECI	
Dopuszczenie lub ignorowanie faktu, że osoby spoza służb informatycznych i telekomunikacyjnych dokonują jakichkolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (hole, korytarze, itp.).	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i ew. opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość. Bezzwłocznie powiadomić administratora bezpieczeństwa informacji (ABI).
Dopuszczanie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość. Bezzwłocznie powiadomić administratora bezpieczeństwa informacji (ABI).

STAROSTA ŁOWICKI

Krzysztof Figat

wzór

Załącznik nr 9
do Polityki bezpieczeństwa przetwarzania danych osobowych w Starostwie Powiatowym w Łowiczu wprowadzonej Zarządzeniem Nr 17/2016
Starosty Łowickiego z dnia 21 marca 2016 r.

REJESTR INCYDENTÓW

L.p./ Data	Imię i nazwisko zgłaszającego	Rodzaj incydentu	Podjęte czynności	Efekt podjętych czynności	Data zamknięcia incydentu	Zatwierdził zamknięcie incydentu
1						
2						
3						
4						
5						

STAROSTA ŁOWICKI
Krzysztof Figat

Załącznik nr 10
do Polityki bezpieczeństwa przetwarzania danych osobowych w Starostwie Powiatowym w Łowiczu wprowadzonej Zarządzeniem Nr ...17/2016.....
Starosty Łowickiego z dnia ..21 marca 2016 r.

REJESTR TWORZENIA KOPII

L.p.	Nazwa systemu lub aplikacji	Lokalizacja jednostki danych	Nazwa serwera	Typ danych (system operacyjny, baza danych, pliki, poczta, inne)	Typ backupu (pełny, przyrostowy, różnicowy)	Wolumen [GB]
1						
2						
3						
4						
5						

L.p.	Nazwa systemu lub aplikacji	Częstotliwość wykonywania backupu	Ilość kopii zapasowych	Sposób wykonywania kopii	Okres przechowywania	Miejsce przechowywania kopii zapasowych	Okno czasowe backupu
1							
2							
3							
4							

STAROSTA ŁOWICKI
Krzysztof Figat

Załącznik nr 2
do Zarządzenia Nr 17/2016
Starosty Łowickiego
z dnia 21 marca 2016 roku

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

w

Starostwie Powiatowym w Łowiczu

Marzec 2016 r.

SPIS TREŚCI

WSTĘP 3

PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM ORAZ WSKAZANIE OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI 5

ZASADY OGÓLNE 6

MODYFIKACJA UPRAWNIEŃ 7

ODEBRANIE UPRAWNIEŃ 8

ZARZĄDZANIE PRZYWILEJAMI 9

ZASADY POSTĘPOWANIA Z HASŁAMI UŻYTKOWNIKÓW UPRZYWILEJOWANYCH . 9

ZASADY OGÓLNE 10

POLITYKA HASEŁ 10

ZASADY POSTĘPOWANIA Z KLUCZAMI KRYPTOGRAFICZNYMI 11

PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU 12

PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA, PROWADZENIA I ZAKOŃCZENIA PRACY W SYSTEMIE INFORMATYCZNYM 13

ZASADY KORZYSTANIA ZE SŁUŻ|\BOWEJ POCZTY ELEKTRONICZNEJ 13

ZASADY KORZYSTANIA Z SIECI PUBLICZNEJ (INTERNET) 14

PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA 15

ZASADY OGÓLNE 16

SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE 18

UŻYTKOWANIE SPRZĘTU KOMPUTEROWEGO, OPROGRAMOWANIA, NOŚNIKÓW DANYCH 18

KORZYSTANIE Z URZĄDZEŃ KOMUNIKACJI GŁOSOWEJ, FAKSOWEJ I WIZYJNEJ 19

SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO.. 20

OCHRONA PRZED SZKODLIWYM OPROGRAMOWANIEM 20

SPOSÓB REALIZACJI WYMOGÓW ODNOTOWANIA INFORMACJI O ODBIORCACH, KTÓRYM DANE OSOBOWE ZOSTAŁY UDOSTĘPNIONE 21

PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH 22

POSTANOWIENIA KOŃCOWE 23

WSTĘP

Niniejsza instrukcja zawiera sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Łowiczu.

Zatwierdzona przez Starostę Łowickiego jest przyjęta do stosowania i stanowi obowiązujący ogół pracowników i współpracowników Starostwa dokument. Zawarte w niej procedury i wytyczne powinny być przekazane osobom odpowiedzialnym w jednostce za ich realizację stosownie do przydzielonych uprawnień, zakresu obowiązków i odpowiedzialności.

Mając na względzie obowiązek stosowania przez Administratora odpowiednich zabezpieczeń systemu informatycznego określonych w art. 36–39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2015 r. poz. 2135), wprowadza się do stosowania środki bezpieczeństwa na poziomie wysokim w rozumieniu rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 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. 2004 nr 100 poz. 1024).

Zależności pomiędzy zakresem przetwarzanych danych i zagrożeniem, na jakie są narażone, a wymaganym poziomem bezpieczeństwa obrazuje rys. nr 1.

Kategorie przetwarzanych danych, rodzaje zagrożeń	⇨	Poziom bezpieczeństwa
W systemie, brak jest danych wrażliwych. System nie jest połączony z siecią publiczną.	➡	**1. podstawowy**
W systemie, przetwarzane są dane wrażliwe. System nie jest połączony z siecią publiczną.	➡	**2. podwyższony**
System jest połączony z siecią publiczną – występują zagrożenia pochodzące z sieci publicznej.	➡	**3. wysoki**

Administrator stosuje wysoki poziom bezpieczeństwa systemu informatycznego, ponieważ systemy używane do przetwarzania danych połączone zostały z siecią wykorzystywaną do świadczenia usług publicznych. Jego zastosowanie jest również niezbędne z uwagi na dodatkowe zagrożenia, jakie mogą pochodzić z sieci publicznej (Internet).

Tabela nr 1

Lp.	OPIS WYMAGANYCH ROZWIĄZAŃ TECHNICZNYCH LUB ORGANIZACYJNYCH
I.	1. Obszar, w którym przetwarzane są dane osobowe zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. 2. Przebywanie osób nieuprawnionych w obszarze w którym przetwarzane są dane osobowe jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
II.	1. W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych. 2. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby: 1) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator; 2) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.
III.	System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed: 1. działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego; 2. utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
IV.	1. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie. 2. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. 3. Kopie zapasowe: 1) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem; 2) usuwa się niezwłocznie po ustaniu ich użyteczność.
V.	Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.
VI.	Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do: 1. likwidacji pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie; 2. przekazania podmiotowi nieuprawnionemu do przetwarzania danych pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie; 3. naprawy pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.
VII.	Administrator monitoruje wdrożone zabezpieczenia systemu informatycznego.
VIII.	W przypadku gdy do uwierzytelniania użytkowników używa się hasła, składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
IX.	Urządzenia i nośniki zawierające dane osobowe wrażliwe (sensytywne), przekazywane poza

	obszar, w którym przetwarzane są dane osobowe, zabezpiecza się w sposób zapewniający poufność i integralność tych danych.
X.	Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, rozszerza się o sposób stosowania środków zabezpieczających urządzenia i nośniki zawierające dane osobowe wrażliwe (sensytywne) przekazywane poza obszar, w którym przetwarzane są dane osobowe zapewniający poufność i integralność tych danych.
XII.	1. System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem. 2. W przypadku zastosowania logicznych zabezpieczeń, o których mowa powyżej, obejmują one: 1) kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną; 2) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.
XIII.	Administrator stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

Wykaz minimalnych środków bezpieczeństwa dla poziomu bezpieczeństwa określonego jako wysoki.

W celu zapewnienia ochrony przetwarzanym danym, w odniesieniu do każdego z wymienionych wyżej punktów, w treści Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych określone zostały zasady postępowania odpowiednie dla stosowanych systemów informatycznych.

PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM ORAZ WSKAZANIE OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, ABI, ASI.
Do wiadomości: Osoby upoważnione.

§1. Niniejszy rozdział opisuje zasady przyznawania użytkownikowi systemu informatycznego identyfikatora, jak również zasady nadawania lub modyfikacji uprawnień dostępu użytkownika do zasobów systemu informatycznego. Zawarte w niniejszym rozdziale procedury obejmują również:

1) operacje związane z nadawaniem użytkownikom uprawnień do pracy w systemie informatycznym począwszy od utworzenia użytkownikowi konta, poprzez przydzielanie i modyfikację jego uprawnień, aż do momentu usunięcia konta z systemu informatycznego;

2) zasady postępowania z hasłami administracyjnymi;

3) zasady administrowania systemem informatycznym w przypadkach awaryjnych (np. w czasie nieobecności Administratora);

4) wskazanie osób odpowiedzialnych za realizację procedury określającej zasady przyznawania uprawnień do korzystania z systemów informatycznych oraz za realizację związanych z tym czynności technicznych takich, jak rejestrowanie i wyrejestrowywanie użytkowników, którym uprawnienia te zostały nadane.

ZASADY OGÓLNE

§2.1. Przydzielanie uprawnień do systemu informatycznego realizowane jest w oparciu o następujące zasady:

1) „Minimalnych przywilejów" – każdy użytkownik posiada prawa dostępu do zasobów ograniczone wyłącznie do tych, które są niezbędne do wykonywania powierzonych mu obowiązków;

2) „Wiedzy koniecznej" – pracownicy posiadają wiedzę o zasobach ograniczoną wyłącznie do zagadnień, które są niezbędne do realizacji powierzonych im zadań;

3) „Domniemanej odmowy" – wszystkie działania, które nie są jawnie dozwolone są zabronione.

2.Dostęp do systemu informatycznego mogą posiadać, w zależności od wykonywanych czynności służbowych lub umownych:

1) pracownicy Administratora w zakresie niezbędnym do właściwego wykonywania obowiązków służbowych;

2) osoby, przy pomocy których Administrator wykonuje swoje czynności, w szczególności:

a. osoby zatrudnione na podstawie umowy cywilnoprawnej,

b. pracownicy lub osoby działające w imieniu podmiotu zewnętrznego świadczącego usługi na rzecz administratora danych,

c. stażyści, na podstawie umowy z Urzędem Pracy,

d. praktykanci, na podstawie umowy ze szkołą wyższą,

e. wolontariusze, na podstawie umowy o wolontariat.

3.Użytkownik systemu informatycznego jest jednoznacznie identyfikowany poprzez nadany mu indywidualny identyfikator użytkownika.

4.Niedopuszczalne jest korzystanie z tego samego identyfikatora przez więcej niż jednego użytkownika.

5.Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi.

6. Uprawnienia dostępu są nadawane wyłącznie w zakresie wynikającym z zajmowanego stanowiska i potrzeby wykonywania obowiązków służbowych na danym stanowisku pracy. Bezzasadne nadawanie uprawnień administratora (przywilejów) będzie kwalifikowane jako incydent związany z bezpieczeństwem informacji.

7.Użytkownikowi systemu informatycznego zostaje nadany dostęp po:

1) zapoznaniu z przepisami dotyczącymi ochrony danych osobowych;

2) zapoznaniu się z niniejszą dokumentacją przetwarzania danych osobowych;

3) podpisaniu oświadczenia o zachowaniu informacji (w tym danych osobowych), do których użytkownik będzie miał dostęp podczas wykonywania obowiązków służbowych lub zobowiązań umownych oraz środków ich zabezpieczania w tajemnicy (również po ustaniu łączącej strony umowy), w tym powstrzymanie się od wykorzystywania ich w celach pozasłużbowych;

4) otrzymaniu upoważnienia do przetwarzania danych osobowych.

8.***Rejestr użytkowników*** wraz z uprawnieniami do systemu lub aplikacji prowadzi administrator systemu informatycznego.

9.Rejestr, o którym mowa powyżej prowadzony jest w postaci elektronicznej lub papierowej.

10.Weryfikację aktualności rejestru, o którym mowa powyżej prowadzi administrator systemu informatycznego we współdziałaniu ze osobami odpowiedzialnymi za wnioskowanie o nadanie/modyfikację/odebranie uprawnień do systemu informatycznego.

11.Administrator systemu informatycznego raz na 30 dni dokonuje przeglądu stanu aktywności kont użytkowników.

NADANIE UPRAWNIEŃ

§3.1. Kierownik użytkownika zobowiązany jest do złożenia wniosku o nadanie uprawnień do systemu informatycznego dotyczącego nadania uprawnień do danego systemu informatycznego administratora danych. Wniosek powinien zawierać poprawną informację o profilu uprawnień (zgodnym z obowiązującym katalogiem profili uprawnień lub przyjętym zakresem obowiązków na danym stanowisku). Wzór wniosku określa załącznik nr 4 ***Wniosek o nadanie uprawnień*** do polityki bezpieczeństwa.

2.Kierownik określając zakres uprawnień, o który wnioskuje dla użytkownika obowiązany jest do stosowania zasad, o których mowa w § 2.

3.Po dopełnieniu powyższych wymagań wniosek powinien zostać przekazany do administratora systemu informatycznego.

4.Administrator systemu informatycznego realizuje otrzymany wniosek lub odmawia nadania uprawnień do systemu informatycznego w przypadku uchybienia wymogom określonym w § 3 ust.7 pkt3 lub powzięciu przed administratora systemu informatycznego podejrzeń co do przekroczenia uprawnień wymaganych na danym stanowisku.

5.W przypadku powzięcia podejrzenia co do przekroczenia uprawnień wymaganych na danym stanowisku, administrator systemu informatycznego jest obowiązany zgłosić ten fakt administratorowi bezpieczeństwa informacji.

6.W przypadku nadania uprawnień wymagających logowania, administrator systemu informatycznego przekazuje użytkownikowi informację zawierającą wymienione z nazwy systemy informatyczne, do których użytkownik otrzymał dostęp oraz login i hasło na potrzeby pierwszego logowania.

7.Wniosek o nadanie uprawnień może zostać sporządzony i przekazany administratorowi systemu informatycznego za pomocą poczty elektronicznej.

MODYFIKACJA UPRAWNIEŃ

§4.1. Bezpośredni przełożony jest zobowiązany do złożenia wniosku o zmianę uprawnień do systemu informatycznego dotyczącego modyfikacji uprawnień do danego zasobu informatycznego. Wzór wniosku określa załącznik nr 4 ***Wniosek o nadanie uprawnień*** do polityki bezpieczeństwa.

2.Wniosek modyfikujący uprawnienia pracownika powinien zostać złożony do administratora systemu informatycznego w możliwie najkrótszym czasie po wystąpieniu zapotrzebowania na dostęp do danego zasobu informatycznego.

3.W zależności od obszaru zmian, wniosek powinien zawierać uzasadnienie wnoszonych zmian oraz informację o przedmiocie modyfikacji:

1) zmiana/Dodanie/Usunięcie uprawnień w profilu uprawnień;

2) przekierowanie skrzynki pocztowej;

3) założenie dodatkowej skrzynki pocztowej;

4) dodanie/Usunięcie Grupy Dystrybucyjnej;

5) dodanie/Usunięcie użytkownika w zakresie członkostwa grupy dystrybucyjnej;

6) zestawienie łącza VPN;

7) nadanie indywidualnych uprawnień do systemów poza zdefiniowanym profilem.

4.Administrator systemu informatycznego realizuje otrzymany wniosek lub odmawia nadania uprawnień do systemu informatycznego w przypadku uchybienia wymogom określonym w §2 ust. 7 pkt 3 lub powzięciu przed administratora systemu informatycznego podejrzeń co do przekroczenia uprawnień wymaganych na danym stanowisku.

5.W przypadku powzięcia podejrzenia co do przekroczenia uprawnień wymaganych na danym stanowisku, administrator systemu informatycznego jest obowiązany zgłosić ten fakt administratorowi bezpieczeństwa informacji.

6.W przypadku nadania uprawnień wymagających logowania, administrator systemu informatycznego przekazuje użytkownikowi informację zawierającą wymienione z nazwy systemy informatyczne, do których użytkownik otrzymał dostęp oraz login i hasło na potrzeby pierwszego logowania.

7.Wniosek o modyfikację uprawnień może zostać sporządzony i przekazany administratorowi systemu informatycznego za pomocą poczty elektronicznej.

ODEBRANIE UPRAWNIEŃ

§5.1. Kierownik jest zobowiązany do złożenia wniosku o odebranie uprawnień do systemu informatycznego dotyczącego odebrania użytkownikowi uprawnień do danego zasobu informatycznego. Wzór wniosku określa załącznik nr 4 ***Wniosek o nadanie uprawnień*** do polityki bezpieczeństwa.

2.Terminami obowiązującymi przy składaniu wniosku są w szczególności:

1) **w przypadku ustania stosunku pracy** – wniosek odbierający wszystkie uprawnienia – natychmiast, najpóźniej ostatniego dnia pracy zatrudnionego;

2) **długotrwałe zwolnienie lekarskie** – wniosek odbierający wszystkie uprawnienia – natychmiast po upływie 30 (trzydziestu) dni kalendarzowych zwolnienia lekarskiego;

3) **zmiana stanowiska pracy** – wniosek odbierający część uprawnień – natychmiast, najpóźniej ostatniego dnia pracy przed zmianą stanowiska na stanowisko wymagające zmniejszenia uprawnień.

3.Po spełnieniu powyższych wymagań wniosek powinien zostać przekazany do administratora systemu informatycznego.

4.Administrator systemu informatycznego przyjmuje wniosek o odebranie uprawnień do systemu informatycznego spełniający wymogi opisane powyżej.

5.Dokonuje weryfikacji poprawności wniosku o odebranie uprawnień do systemu informatycznego.

6.Administrator systemu informatycznego bezzwłocznie realizuje otrzymany wniosek.

7.Wniosek o odebranie uprawnień może zostać sporządzony i przekazany administratorowi systemu informatycznego za pomocą poczty elektronicznej.

ZARZĄDZANIE PRZYWILEJAMI

§6.1.Nadawane przywileje (większe uprawnienia niż wynika to z realizowanych rutynowych zadań użytkownika) podlegają ścisłej ewidencji prowadzonej przez administratora systemu informatycznego.

2.Przywileje w systemie nadaje administrator systemu informatycznego.

3.Uprzywilejowane konto nie może służyć do realizacji przez użytkownika rutynowych zadań.

4.Przywileje podlegają cofnięciu niezwłocznie po ustaniu potrzeby uzasadniającej ich nadanie.

5.Nadawane przywileje podlegają regularnym przeglądom i kontroli.

ZASADY POSTĘPOWANIA Z HASŁAMI ADMINISTRACYJNYMI

§7.1W stosunku do haseł użytkowników uprzywilejowanych stosuje się zaostrzone standardy bezpieczeństwa.

2.Standardy, o których mowa powyżej stosuje się również do haseł:

1) elementów aktywnych sieci teleinformatycznych;

2) konfiguracji komputerów, w tym hasła do BIOS.

3.Hasła, o których mowa w ust. 1 i 2 przechowuje się w postaci zaszyfrowanej.

4.Do przechowywania haseł zapisanych na papierze stosuje się wyłącznie koperty, które uniemożliwiają otwarcie bez uszkodzenia ich struktury (tzw. „koperty bezpieczne").

5.Koperty z hasłami przechowuje się w sejfie, w miejscu zapewniającym dostęp tylko osobom upoważnionym. Dane umieszczone na bezpiecznej kopercie zawierają:

1) numer koperty adekwatny do numeru ewidencyjnego podanego w ewidencji haseł;

2) datę jej złożenia i podpis osoby składającej kopertę;

3) skróconą nazwę przynależności hasła.

6.Koperty z hasłami podlegają ścisłej ewidencji prowadzonej przez administratora systemu informatycznego.

7.Ewidencja haseł przechowywana jest w miejscu zabezpieczonym przed dostępem osób niepowołanych.

8.Za aktualność przechowywanych haseł odpowiedzialny jest administrator systemu informatycznego.

9.Awaryjne otwarcie bezpiecznej koperty oraz pobranie kopii hasła znajdującego się w kopercie wymaga uprzedniej pisemnej akceptacji Administratora lub osoby przez niego upoważnionej i jest udokumentowane w ewidencji kopert.

10.Po użyciu, hasło ulega zniszczeniu, a w to miejsce jest generowane nowe hasło, którego kopia jest przechowywana na identycznych zasadach jak w przypadku zniszczonego hasła.

STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

Zakres przedmiotowy stosowania:

Podmioty obowiązane do stosowania: Administrator, ABI, ASI, osoby upoważnione

§8. W Niniejszy rozdział reguluje tryb przydzielania haseł, wymogi dotyczące stopnia ich złożoności oraz wskazuje osoby odpowiedzialne za przydział haseł. Zawarte w niniejszym rozdziale procedury odnoszą się również do:

1) możliwych zagrożeń i konsekwencji związanych z tzw. utratą tożsamości elektronicznej (tj. utratą danych służących uwierzytelnieniu, co może skutkować pozyskaniem tych danych przez osoby nieuprawnione);

2) zalecanych sposobów korzystania z przeglądarek internetowych.

ZASADY OGÓLNE

§9.1. Każdy użytkownik systemu informatycznego musi posiadać unikalny identyfikator i wprowadzone przez siebie hasło autoryzujące jego osobę w systemie informatycznym.

2.Hasła użytkowników lub inne dane uwierzytelniające podlegają szczególnej ochronie.

3.Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła (prócz pierwszego hasła do systemu nadawanego przez administratora systemu informatycznego) i jego przechowywanie.

4.Osoba pełniąca funkcję administratora systemu powinna posiadać dodatkowo odrębne konto służące tylko i wyłącznie do administracji danym systemem informatycznym o ile dany system udostępnia taką funkcjonalność.

POLITYKA HASEŁ

§10. Każdy użytkownik posiadający dostęp do systemów informatycznego Administratora jest obowiązany do:

1)zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystanych do pracy w systemie informatycznym;

2) niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia;

3) niezwłocznej zmiany hasła tymczasowego, przekazanego przez administratora systemu informatycznego;

4) poinformowania administratora systemu informatycznego oraz administratora bezpieczeństwa informacji o podejrzeniu lub rzeczywistym ujawnieniu hasła;

5) stosowania haseł o minimalnej długości 8 znaków, zawierających kombinację małych i dużych liter oraz cyfr lub znaków specjalnych;

6) stosowania haseł nie posiadających w swojej strukturze części loginu;

7) stosowania haseł nie będących zbliżonymi do poprzednich (np. Tadeusz$2013 - Tadeusz$2014),

8) zmiany wykorzystywanych haseł **raz na 30 dni.**

§11.1. Hasła zachowują swoją poufność również po ustaniu ich użyteczności.

2.Zabronione jest:

1) zapisywanie haseł w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób;

2) stosowanie haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania
z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.;

3) używanie tych samych haseł w różnych systemach operacyjnych i aplikacjach;

4) udostępnianie haseł innym użytkownikom;

5) przeprowadzanie prób łamania haseł;

6) wpisywanie haseł „na stałe" (np. w skryptach logowania) oraz wykorzystywania opcji auto-zapamiętywania haseł (np. w przeglądarkach internetowych).

§12.1Administrator systemu informatycznego obowiązany jest do skonfigurowania systemu, aby próby dostępu do tego systemu były limitowane zarówno w ujęciu ilościowym, jak i czasowym jeżeli system umożliwia wymienioną konfigurację.

2.W przypadku, gdy system umożliwia limitowanie wprowadzenia błędnego hasła, należy przyjąć próg ilości wprowadzonych błędnych haseł na 3, po czym ustanowić blokadę konta.

3.Należy ograniczyć możliwość wielokrotnego logowania, gdzie użytkownik loguje się na kilku komputerach równocześnie wykorzystując ten sam identyfikator.

4.Administrator systemu informatycznego odblokowuje/ zresetuje hasło do danego systemu informatycznego w przypadku przekroczenia przez użytkownika ustalonej ilości prób logowania.

5.Po dokonaniu czynności przez administratora systemu informatycznego stosowną informacja o odblokowaniu dostępu do konta użytkownika zostanie przekazana użytkownikowi.

ZASADY POSTĘPOWANIA Z KLUCZAMI KRYPTOGRAFICZNYMI

§13.1W systemach obsługujących transmisję danych osobowych wrażliwych lub informacji poufnych Administratora powinny być wykorzystywane klucze kryptograficzne służące do zabezpieczenia danych. W celu kontroli użytkowników jest prowadzony Rejestr

kluczy kryptograficznych. Rejestr zawiera informację dot. użytkownika, w tym imię i nazwisko, stanowisko, data otrzymania klucza.

2.Za generowanie, przechowywanie i bezpieczną dystrybucję kluczy kryptograficznych odpowiada administrator systemu informatycznego.

3.Przekazywanie kluczy użytkownikom powinno odbywać się w sposób protokolarny, o ile nie następuje w drodze teletransmisji. Rejestr o którym mowa w ust.1wraz z ewentualnymi protokołami jest prowadzony przez ASI i stanowi dokumentację Klucz kryptograficzny.

4.Obowiązkiem użytkownika jest zabezpieczenie kluczy (prywatnych) przed dostępem osób nieupoważnionych.

5.W przypadku stwierdzenia ujawnienia klucza osobie nieupoważnionej lub podejrzenia jego ujawnienia, należy bezzwłocznie powiadomić administratora systemu informatycznego oraz administratora bezpieczeństwa informacji.

6.Dane osobowe wrażliwe lub informacje poufne Administratora , do których nie stosuje się kluczy kryptograficznych, można przesyłać wyłącznie pocztą elektroniczną po uaktywnieniu funkcji podpisywania i szyfrowania pliku.

7.Każdy użytkownik korzystający z kluczy kryptograficznych jest zobowiązany do ich użytkowania i przechowywania w sposób uniemożliwiający utratę lub dostęp osób niepowołanych.

8.W przypadku podejrzenia lub rzeczywistego naruszenia bezpieczeństwa klucza fakt ten należy niezwłocznie zgłosić administratorowi systemu informatycznego oraz administratorowi bezpieczeństwa informacji.

PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, ABI, ASI, osoby upoważnione

§14. Niniejszy rozdział opisuje kolejne czynności, jakie należy wykonać w celu uruchomienia systemu informatycznego, a w szczególności zasady postępowania użytkowników podczas przeprowadzania procesu uwierzytelniania się (logowania się do systemu). Przestrzeganie określonych w instrukcji zasad ma na celu zachowanie poufności haseł oraz uniemożliwienie nieuprawnionego przetwarzania danych. Zawarte w niniejszym rozdziale procedury obejmują również:

1) metody postępowania w sytuacji tymczasowego zaprzestania pracy na skutek opuszczenia stanowiska pracy,

2) metody postępowania w sytuacji , kiedy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba,

3) sposób postępowania w sytuacji podejrzenia naruszenia bezpieczeństwa systemu, np. w razie braku możliwości zalogowania się użytkownika na jego konto czy też w sytuacji

stwierdzenia fizycznej ingerencji w przetwarzane dane bądź użytkowane narzędzia programowe lub sprzętowe.

PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA, PROWADZENIA I ZAKOŃCZENIA PRACY

§15.1Rozpoczęcie pracy w systemie informatycznym następuje po wprowadzeniu unikalnego identyfikatora i hasła.

2.Zawieszenie pracy w systemie informatycznym tj. brak wykonywania jakichkolwiek czynności przez okres **5 minut** w systemie informatycznym powoduje automatycznie uruchomienie systemowego wygaszacza ekranu blokowanego hasłem.

3.Przed zakończeniem pracy należy upewnić się czy dane zostały zapisane, aby uniknąć utraty danych.

4.Przed opuszczeniem miejsca pracy, użytkownik obowiązany jest wylogować się z systemu informatycznego przetwarzającego dane osobowe i z systemu operacyjnego, zabezpieczyć nośniki informacji (elektroniczne i papierowe) oraz wyłączyć komputer.

5.W sytuacji gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlaną treść.

6.Użytkownik systemu informatycznego przetwarzającego dane osobowe niezwłocznie powiadamia administratora systemu w przypadku, gdy:

1) wygląd systemu, sposób jego działania, zakres danych lub sposób ich przedstawienia przez system informatyczny odbiega od standardowego stanu uznawanego za typowy dla danego systemu informatycznego;

2) niektóre opcje, dostępne użytkownikowi w normalnej sytuacji, przestały być dostępne lub też opcje niedostępne użytkownikowi w normalnej sytuacji, stały się dostępne.

ZASADY KORZYSTANIA ZE SŁUŻBOWEJ POCZTY ELEKTRONICZNEJ

§16.1. Użytkownikowi zostaje nadany dedykowany adres skrzynki poczty elektronicznej działający w domenie administratora danych.

2.Informacja o służbowym adresie skrzynki pocztowej jest jawna i dostępna powszechnie, w tym może być dostępna na łamach witryny internetowej administratora danych w postaci książki adresowej.

3.Nadany użytkownikowi adres skrzynki poczty elektronicznej służy wyłącznie do realizacji celów służbowych lub umownych. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów informatycznych administratora danych podlega rejestrowaniu i może być monitorowana. Informacje przesyłane za pośrednictwem sieci administratora danych (w tym do i z Internetu) nie stanowią własności prywatnej użytkownika.

4.Wszelka korespondencja elektroniczna niezwiązana z działalnością administratora danych, powinna być prowadzona przez prywatną skrzynkę poczty elektronicznej użytkownika.

5.Korzystanie z systemu poczty elektronicznej dla celów prywatnych nie może wpływać na wydajność systemu poczty elektronicznej. Użytkownicy mogą korzystać z systemu poczty elektronicznej dla celów prywatnych wyłącznie incydentalnie.

6.Użytkownicy dokonujący wysyłki korespondencji masowej poza organizację, obowiązani są do ukrywania odbiorów w kopii (pole BCC lub UDW).

7.Zabronione jest:

1) wysyłanie materiałów służbowych na konta prywatne (np. celem pracy nad dokumentami w domu);
2) wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić wizerunkowi administratora danych,
3) odbieranie przesyłek z nieznanych źródeł;
4) otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.;
5) przesyłanie pocztą elektroniczną plików wykonywalnych typu: bat, com, exe, plików multimedialnych oraz plików graficznych;
6) ukrywanie lub dokonywanie zmian tożsamości nadawcy;
7) czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika;
8) odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem; w przypadku otrzymania takiej wiadomości należy przesłać ją administratorowi systemu informatycznego;
9) posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy lub obowiązków umownych;
10) wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb administratora danych lub do poszukiwania dodatkowego zatrudnienia.

ZASADY KORZYSTANIA Z SIECI PUBLICZNEJ (INTERNET)

§17.1. Sieć, w której pracują urządzenia komputerowe Administratora musi być odseparowana od sieci publicznej zaporą ogniową oraz systemem wykrywania włamań (IPS).

2.Zdalne korzystanie z systemów informatycznych poprzez sieć publiczną może mieć miejsce po zastosowaniu systemu uwierzytelniania użytkownika i szyfrowanego kanału transmisji.

3.Zdalny dostęp do serwerów w celach administracyjnych może mieć miejsce po zastosowaniu systemu uwierzytelniania użytkownika i szyfrowanego kanału transmisji.

4.Systemy informatyczne powinny korzystać z szyfrowanych protokołów wymiany danych,
w szczególności połączeń sftp i https.

5.Dostęp użytkowników do sieci publiczne (Internet) powinien być ograniczony do niezbędnego minimum na danym stanowisku pracy.

6.Dostęp do przeglądania stron internetowych możliwy jest po nadaniu odpowiednich uprawnień (USER, VIP, GUEST).

7.Wprowadza się całkowite ograniczenia w dostępie do treści uznanych za pornograficzne, rasistowskie, traktujące o przemocy, przestępstwach, jak również do protokołów umożliwiających wymianę plików w sieciach z naruszeniem przepisów prawa.

8.Dostęp do protokołu wymiany plików możliwy jest w uzasadnionych przypadkach, po nadaniu odpowiednich uprawnień.

9.Dalsze ograniczenia dostępu do sieci Internet mogą być rekomendowane przez administratora bezpieczeństwa informacji.

10.Wszelkie odstępstwa od reguł określonych w ust. 1 - 4 możliwe są po uzyskaniu zgody administratora danych.

ZASADY POSTĘPOWANIA Z NOŚNIKAMI ELEKTRONICZNYMI ORAZ VPN PODCZAS PRACY POZA OBSZAREM PRZETWARZANIA DANYCH

§18. Każdy użytkownik wymiennych nośników elektronicznych oraz użytkownicy zdalnych dostępów do sieci służbowej Administratora (VPN) oraz użytkownicy elektronicznych kart dostępu ponoszą całkowitą odpowiedzialność za powierzony do użytkowania sprzęt oraz są obowiązani do stosowania się do poniższych zasad:

1) zabrania się pozostawiania bez opieki w miejscach publicznych nośników wymiennych przetwarzających informacje Administratora;

2) komputery przenośne należy przewozić jako bagaż podręczny i w miarę możliwości je maskować;

3) użytkownik wykonując czynności zawodowe lub umowne w domu powinien zadbać o należyte zabezpieczenie powierzonego sprzętu oraz dostępu do informacji przed nieautoryzowanym dostępem osób trzecich;

4) zabrania się spożywania posiłków i picia podczas pracy z powierzonym sprzętem,

5) zabrania się udostępniania osobom trzecim nośników elektronicznych informacji oraz powierzonego sprzętu będącego własnością Administratora;

6) w przypadku utraty nośnika elektronicznego lub sprzętu komputerowego należy ten fakt bezzwłocznie zgłosić do bezpośredniego przełożonego administratora bezpieczeństwa informacji lub administratora systemu informatycznego. Bezpośredni przełożony lub administrator systemu informatycznego bezzwłocznie zgłaszają taki fakt do administratora bezpieczeństwa informacji, ponieważ zagubienie nośnika przetwarzającego dane może wiązać się z utratą poufności informacji chronionych przez Administratora;

7) problemy wynikające z nieprawidłowego funkcjonowania sprzętu komputerowego należy zgłaszać administratorowi systemu informatycznego.

PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

Zakres przedmiotowy stosowania:

Podmioty obowiązane do stosowania: Administrator, ABI, ASI, osoby upoważnione

Do wiadomości: osoby upoważnione

§19. Niniejszy rozdział opisuje metody i częstotliwość tworzenia kopii zapasowych danych oraz kopii zapasowych systemu informatycznego używanego do ich przetwarzania. Zawarte w niniejszym rozdziale procedury obejmują również:

1) określenie, dla jakich danych wykonywane będą kopie zapasowe, typ nośników, na których będą one wykonywane oraz narzędzia programowe i urządzenia, które mają być do tego celu wykorzystywane;
2) harmonogram wykonywania kopii zapasowych dla poszczególnych zbiorów danych wraz ze wskazaniem odpowiedniej metody sporządzania kopii.

ZASADY OGÓLNE

§20.1. Kopie zapasowe systemów, aplikacji baz danych i dokumentów użytkowanych przez Administratora służą do zapewnienia możliwości odtworzenia w przypadku utraty aktualnie użytkowanych danych i/lub konfiguracji systemów i aplikacji.

2.Za tworzenie kopii zapasowych i archiwalnych odpowiedzialny jest administrator systemu informatycznego.

3.Tworzenie kopii odbywa się zgodnie z procedurą tworzenia i odtwarzania kopii zapasowych i podlega rejestracji. Wzór rejestru określa załącznik nr 10 ***Rejestr tworzenia kopii*** do Polityki bezpieczeństwa. Rejestr prowadzony jest w postaci papierowej lub elektronicznej.

4.Po utworzeniu kopii automatycznie (jeżeli jest technicznie realizowalne) jest generowany raport o przebiegu wykonania kopii. Raport podlega weryfikacji przez administratora systemu informatycznego.

5.Miejsce przechowywania kopii jest zabezpieczone przed nieuprawnionym dostępem oraz skutkami zdarzeń takich, jak pożar, zalanie, oddziaływanie silnego pola elektromagnetycznego, promieniowanie, zanieczyszczenie środowiska na takim poziomie, jak jest zabezpieczony system, z którego kopia zapasowa została wykonana.

6.Kopie są przechowywane w bezpiecznej odległości (w innej lokalizacji) od miejsca, w którym jest prowadzona eksploatacja systemów.

7.Regularnie, co najmniej dwa razy w roku, administrator systemu informatycznego przeprowadza testowe sprawdzenie odtworzenia systemu, aplikacji, bazy danych lub dokumentów z kopii. Testowe odtworzenie podlega udokumentowaniu w dzienniku pracy systemu jeżeli jest prowadzone.

8.W przypadku, gdy okres trwałości zapisu na nośniku elektronicznym lub magnetycznym jest krótszy od wymaganego okresu przechowywania wynikającego z uwarunkowań prawnych dane z nośników są przenoszone na inny nośnik.

9.Nośnik, z którego przeniesiono zapis, jest niszczony zgodnie z zasadami obowiązującymi u Administratora.

10.Po upływie wymaganego okresu przechowywania kopie archiwalne są niszczone zgodnie z zasadami obowiązującymi u Administratora.

ZASADY TWORZENIA KOPII BEZPIECZEŃSTWA I KOPII ARCHIWALNYCH

§21.1. Zbiory danych, oprogramowanie oraz konfiguracja systemów operacyjnych serwerów Administratora powinny być zabezpieczone w postaci cyklicznie wykonywanych kopii bezpieczeństwa lub archiwalnych.

2.Kopie bezpieczeństwa należy wykonywać:

1) przed dokonaniem zmian w konfiguracji systemów operacyjnych lub oprogramowania;
2) przed dokonaniem zmian w programach (np. zmiana wersji);
3) przed i/lub po każdej istotnej zmianie danych w bazie danych.

3.Oprócz kopii, o których mowa w ust. 2., należy wykonywać kopie archiwalne:

1) miesięczne – na koniec danego miesiąca;
2) roczne – na koniec danego roku.

4.Pliki użytkowników systemu informatycznego powinny być przechowywane na indywidualnie udostępnionych dyskach serwerów.

5.Dyski serwerów, o których mowa w ust. 4 zabezpiecza się przed utratą danych w postaci kopii bezpieczeństwa i/lub archiwalnych.

6.Kopie bezpieczeństwa należy:

1) wykonać w co najmniej dwóch egzemplarzach każdą, przy czym przynajmniej jedną na nośniku wymiennym;
2) przechowywać w dwóch różnych miejscach innych niż te, w którym eksploatowane zbiory przechowywane są na bieżąco (co najmniej w innej strefie pożarowej).

7.Kopie archiwalne należy:

1) wykonać w co najmniej dwóch egzemplarzach każdą na osobnych nośnikach wymiennych;
2) przechowywać w miejscach innych niż te, w których przechowywane są zbiory eksploatowane na bieżąco, przy czym jedną z kopii należy przechowywać poza siedzibą jednostki organizacyjnej;
3) w trakcie transportu zabezpieczyć przed osobami nieupoważnionymi i niekorzystnymi zjawiskami fizycznymi mogącymi doprowadzić do ich zniszczenia bądź uszkodzenia.

8.Kopie bezpieczeństwa należy przechowywać do momentu wykonania następnej kopii bezpieczeństwa.

9.Kopie archiwalne miesięczne należy przechowywać przez okres 1 roku, a kopie roczne przez okres 5 lat, licząc od pierwszego dnia roku następującego po roku, za który wykonana jest kopia.

10.Informacje przychodzące pocztą elektroniczną powinny być zabezpieczone przez użytkownika na udostępnionym dysku serwera plikowego.

SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, ABI, ASI, osoby upoważnione
Do wiadomości: osoby upoważnione

§22. Niniejszy rozdział opisuje sposób i czas przechowywania wszelkiego rodzaju nośników informacji (dyskietki, płyty CD, taśmy magnetyczne) wykorzystywanych przez Administratora. Zawarte w niniejszym rozdziale procedury obejmują również:

1) zdefiniowanie pomieszczeń przeznaczonych do ich przechowywania;
2) sposoby ich zabezpieczenia przed nieuprawnionym przejęciem, odczytem, skopiowaniem lub zniszczeniem.

UŻYTKOWANIE SPRZĘTU KOMPUTEROWEGO, OPROGRAMOWANIA, NOŚNIKÓW DANYCH

§23.1. Do sprzętu komputerowego zalicza się między innymi:

1) komputery stacjonarne;
2) komputery przenośne;
3) Tablety;
4) Smartphony;
5) Drukarki;
6) Modemy;
7) Monitory;
8) Routery;
9) osprzęt dostarczony razem z wyżej wymienionym sprzętem lub zakupiony oddzielnie, a w szczególności: zasilacze, torby, klawiatury, myszki komputerowe.

2.Administrator systemu informatycznego odpowiada za poprawne działanie sprzętu komputerowego. Czynność tą administrator systemu informatycznego może wykonywać poprzez pracowników lub współpracowników Administratora lub poprzez podmioty zewnętrzne.

3.W przypadku wykorzystywania urządzeń mobilnych (m.in. tablet, smartphone) wymaga się zastosowania następujących środków bezpieczeństwa:

1)blokada ekranu (pin/hasło/symbol graficzny);
2)szyfrowanie pamięci/karty pamięci;
3)program antywirusowy;
4)wyłączanie nieużywanych usług (wi-fi, gprs/lte, bluetooth, nfc);
5)instalowanie oprogramowania z zaufanego źródła (np. iStore, Google Play);
6)używanie szyfrowania, np.: poczty lub VPN podczas korzystania z publicznych hotspot–ów.

4. Przekazanie sprzętu jest to czynność polegająca na dostarczeniu sprzętu komputowego wraz z odpowiednim oprogramowaniem użytkownikowi.

5.Administrator systemu informatycznego odpowiedzialny jest za przygotowanie sprzętu komputerowego do prawidłowej i zgodnej z przeznaczeniem pracy.

6.Administrator systemu informatycznego jest zobowiązany do prowadzenia spisu posiadanego pod opieką sprzętu komputerowego oraz oprogramowania wraz z dostarczoną dokumentacją.

7.Administrator systemu informatycznego ma obowiązek przechowywać karty gwarancyjne, klucze i licencje do oprogramowania.

8.Administrator systemu informatycznego prowadzi rejestr wydanego sprzętu komputerowego wraz z wyszczególnieniem użytkownika. Administrator udziela pomocy użytkownikowi w obsłudze sprzętu i oprogramowania.

9.W przypadku niepoprawnego i niezgodnego z przeznaczeniem użytkowania przez użytkownika sprzętu komputerowego, administrator systemu informatycznego informuje o powyższym administratora bezpieczeństwa informacji.

10.Administrator ma prawo instalować wyłącznie licencjonowane oprogramowanie lub oprogramowanie, które nie wymaga opłaty licencyjnej, zgodnie z warunkami licencji.

11.Użytkownik jest zobowiązany do dbałości o sprzęt oraz oprogramowanie, a także odpowiedzialny za zabezpieczenie go przed używaniem przez osoby nieuprawnione oraz do ochrony przed kradzieżą lub zagubieniem.

12.Użytkownik nie może samodzielnie zmieniać konfiguracji przekazanego sprzętu komputerowego oraz instalować lub usuwać oprogramowania, w tym nie może używać na przekazanym sprzęcie prywatnego oprogramowania.

13.Użytkownik nie może udostępniać powierzonego mu sprzętu służbowego, w szczególności urządzeń mobilnych, osobom trzecim.

KORZYSTANIE Z URZĄDZEŃ KOMUNIKACJI GŁOSOWEJ, FAKSOWEJ I WIZYJNEJ

§24.1. Każdy użytkownik zobowiązany jest do przestrzegania zakazu prowadzenia rozmów, podczas których może dochodzić do wymiany informacji danych osobowych lub informacji poufnych u Administratora, jeśli rozmowy te odbywają się w miejscach publicznych, otwartych pomieszczeniach biurowych lub takich, które nie gwarantują zachowania poufności rozmów.

2.Odczytanie wiadomości z faksów, automatycznych sekretarek lub systemów poczty głosowej powinno być możliwe wyłącznie po wprowadzeniu indywidualnego hasła. W przypadku braku takiej możliwości urządzenia należy zabezpieczyć przed dostępem osób nieuprawnionych.

3.Zabronione jest wykorzystywanie domyślnych („fabrycznych") haseł dla ww. urządzeń.

4.Przekazywanie za pomocą urządzeń faksowych dokumentów zawierających dane osobowe wrażliwe lub informacje poufne u Administratora jest zabronione.

5.Drukarki nie mogą być pozostawione bez kontroli, jeśli są wykorzystywane (lub wkrótce będą) do drukowania dokumentów zawierających informacje wrażliwe.

ZABEZPIECZENIE SYSTEMU INFORMATYCZNEGO PRZED UTRATĄ DANYCH SPOWODOWANĄ AWARIĄ ZASILANIA LUB ZAKŁÓCENIAMI W SIECI ZASILAJĄCEJ

§25.1. Wszystkie krytyczne systemy informatyczne powinny być zasilane z wydzielonej sieci oraz zabezpieczone przed krótkotrwałymi zanikami napięcia, przepięciami itp., przy pomocy zasilaczy awaryjnych (UPS).

2.Serwery krytycznych systemów informatycznych winny posiadać niezależne źródła zasilania (generatory) włączane na wypadek zaniku napięcia.

3.Minimalny czas podtrzymywania zasilania za pomocą zasilaczy awaryjnych nie może być krótszy niż:

1) 15 minut dla stacji roboczych;

2) 45 minut dla serwerów.

4.Dopuszcza się krótsze okresy niż określone w ust. 3., jeśli źródła określone w pkt. 2. posiadają funkcje automatycznego uruchomienia.

SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

Zakres przedmiotowy stosowania: Podmioty obowiązane do stosowania: Administrator, ABI, ASI Do wiadomości: osoby upoważnione

§26. Niniejszy rozdział opisuje sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego wraz ze zdefiniowaniem obszaru systemu informatycznego narażonego na ingerencję wirusów komputerowych oraz wszelkiego rodzaju innego szkodliwego oprogramowania. Zawarte w niniejszym rozdziale procedury obejmują również:

1)zdefiniowane źródła przedostania się szkodliwego oprogramowania do systemu oraz działania, jakie należy podejmować, aby minimalizować możliwość jego zainstalowania się;

2)zastosowane narzędzia programowe, których zadaniem jest przeciwdziałanie skutkom szkodliwego oprogramowania;

3)metody i częstotliwość aktualizacji definicji wirusów oraz osoby odpowiedzialne za zarządzanie oprogramowaniem antywirusowym;

4)sposób postępowania użytkowników na okoliczność zidentyfikowania zagrożeń.

OCHRONA PRZED SZKODLIWYM OPROGRAMOWANIEM

§27.1. Zidentyfikowanymi obszarami systemu informatycznego Administratora narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania są dyski twarde lub karty pamięci urządzeń, pamięć RAM oraz elektroniczne nośniki informacji.

2.Drogą przedostania się wirusów lub szkodliwego oprogramowania może być sieć publiczna, wewnętrzna sieć teleinformatyczna lub elektroniczne nośniki informacji.

3.Stacje robocze, komputery przenośne oraz serwery objęte są ochroną w czasie rzeczywistym za pomocą oprogramowania antywirusowego oraz zapory (firewall), zapewniających integralność zasobów przechowywanych i przetwarzanych w systemie informatycznym Administratora.

4.Za prawidłowe funkcjonowanie oprogramowania antywirusowego odpowiada administrator systemu informatycznego.

5.Oprogramowanie antywirusowe uruchamiane jest przy starcie systemu, a użytkownik nie posiada uprawnień do jego wyłączenia.

6.Konfiguracja programu antywirusowego zapewnia ciągłe monitorowanie otrzymywanych
i wysyłanych, a także uruchamianych plików pod kątem występowania oprogramowania złośliwego.

7.Stacje robocze i komputery przenośne przynajmniej raz w miesiącu skanowane są pod kątem występowania na nich oprogramowania złośliwego.

8.Serwery plikowe podlegają skanowaniu pod kątem występowania na nich oprogramowania złośliwego przynajmniej raz w tygodniu.

9.Użytkownicy systemu mają obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.

10.W przypadku stwierdzenia pojawienia się wirusa i braku możliwości usunięcia go przez program antywirusowy, użytkownik powinien skontaktować się z administratorem systemu informatycznego.

11.W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, administrator systemu informatycznego podejmuje działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:

1) usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego;

2) odtworzenie plików z kopii zapasowych, po uprzednim sprawdzeniu, czy dane zapisane na kopiach zapasowych nie są zainfekowane;

3) samodzielną ingerencję w zawartość pliku – w zależności od posiadanych kwalifikacji lub skonsultowanie się z odpowiednim serwisem.

SPOSÓB REALIZACJI WYMOGÓW ODNOTOWANIA INFORMACJI O ODBIORCACH, KTÓRYM DANE OSOBOWE ZOSTAŁY UDOSTĘPNIONE

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, ABI, ASI
Do wiadomości: osoby upoważnione

§28. Dla każdej osoby, której dane osobowe przetwarzane są w systemie informatycznym, system ten powinien zapewnić odnotowanie informacji o udostępnieniach danych odbiorcom,

w rozumieniu art. 7 pkt 6 ustawy, zawierające informacje komu, kiedy i w jakim zakresie dane osobowe zostały udostępnione.

PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: Administrator, ABI, ASI
Do wiadomości: osoby upoważnione

§29.1. Niniejszy rozdział określa cel, zakres, częstotliwość oraz procedury wykonywania przeglądów i konserwacji systemu informatycznego oraz podmioty i osoby do tego uprawnione.
2.Zawarte w niniejszym rozdziale procedury obejmują również:

1) sposób nadzoru nad osobami spoza organizacji wykonującymi czynności konserwacyjne systemu;
2) tryb przekazywania sprzętu komputerowego do naprawy lub zniszczenia.

3.Konserwacja sprzętu komputerowego, systemów informatycznych oraz nośników informacji Administratora ma na celu zapewnienie nieprzerwanej i bezpiecznej pracy tych systemów, zapobieganie utraty, uszkodzenia lub naruszenia bezpieczeństwa.

4.Sprzęt podlega konserwacji według ustalonego planu, wynikającego z zaleceń producentów.

Wszelkie naprawy oraz konserwacje urządzeń komputerowych oraz zmiany w systemie informatycznym Administratora przeprowadzane są – o ile to możliwe – przez upoważnionych pracowników Administratora .

5.Naprawy, konserwacje i zmiany w systemie informatycznym Administratora przeprowadzane przez serwisanta zewnętrznego prowadzone są pod nadzorem administratora systemu informatycznego w siedzibie Administratora (jeśli to możliwe) lub poza siedzibą Administratora, po uprzednim usunięciu elementów zawierających dane osobowe, o ile nie wiąże się to z nadmiernymi utrudnieniami.

6.Wszelkie prace, o których mowa powyżej, wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie pomiędzy Administratorem a tymże podmiotem, z uwzględnieniem klauzuli powierzenia przetwarzania danych lub klauzuli dotyczącej zachowania w poufności przez wykonawcę wszelkich informacji, do których ma dostęp w czasie wykonywania usługi.

7.W przypadku zdalnej obsługi serwisowej systemów informatycznych Administratora, porty komunikacyjne powinny być włączane jedynie na wyraźne żądanie dostawcy takich usług, za zgodą administratora systemu informatycznego i muszą być ponownie odłączone tuż po zakończeniu prac serwisowych.

8.Jeśli nośnik danych (dysk, płyta lub inne) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć mechanicznie w niszczarce spełniającej wymagania normy DIN 66399 na poziomie bezpieczeństwa nie niższym niż 3.

POSTANOWIENIA KOŃCOWE

§30.1. Dokumentacja przetwarzania danych osobowych stanowi wewnętrzną regulację Administratora i obowiązuje wszystkich pracowników i współpracowników Administratora.

2.Dokumentacja przetwarzania danych osobowych obowiązuje od dnia jej wprowadzenia w życie w sposób przyjęty u Administratora. Wszelkie zmiany Dokumentacji przetwarzania danych osobowych obowiązują od dnia ich wprowadzenia w życie w sposób przyjęty u Administratora.

3.Każdy kto przetwarza dane posiadane przez Administratora zobowiązany jest do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Dokumentacji przetwarzania danych osobowych.

4.Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.

5.W sprawach nieuregulowanych w niniejszej instrukcji zarządzania mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy ustawy.

STAROSTA OWICKI

Krzysztof Figat