Załącznik do
Polecenia służbowego nr ……
Dyrektora Zarządu Mienia Skarbu
Państwa
z dnia ……..

Polityka bezpieczeństwa przetwarzania i ochrony danych osobowych oraz Instrukcja zarządzania systemami informatycznymi

I. POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA I OCHRONY DANYCH OSOBOWYCH 4

1. POSTANOWIENIA OGÓLNE……. 4
2. DEFINICJE…… 5
3. ZASADY OCHRONY DANYCH OSOBOWYCH…….…. 8
4. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH……..... 9
5. UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH…... 10
6. ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH……..... 12
7. PRZETWARZANIE SZCZEGÓLNYCH KATEGORII DANYCH OSOBOWYCH……... 12
8. PRZETWARZANIE DANYCH OSOBOWYCH DOTYCZĄCYCH WYROKÓW SKAZUJĄCYCH……. 13
9. MINIMALIZACJA……. 13
10. PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH 13
11. ZARZĄDZANIE RYZYKIEM…….. 14
12. OCENA SKTUKÓW DLA OCHRONY DANYCH……. 14
13. ZASADY PRYWATNOŚCI W FAZIE PROJEKTOWANIA I W USTAWIENIACH DOMYŚLNYCH…… 14
14. REJESTR CZYNNOŚCI PRZETWARZANIA……. 15
15. REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA…….. 15
16. OBSZARY PRZETWARZANIA DANYCH OSOBOWYCH…….. 15
17. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH ORAZ UDOSTĘPNIANIE……. 17
18. WSPÓŁADMINISTRATORZY……. 17
19. OBOWIĄZEK INFORMACYJNY…… 18
20. ODPOWIEDZIALNOŚĆ…… 19
21. REALIZACJA ŻĄDAŃ OSÓB, KTÓRYCH DANE DOTYCZĄ…… 21
22. POSTĘPOWANIE W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH……... 22

23. ŚRODKI OCHRONY DANYCH…….. 24

24. MONITOROWANIE POSTANOWIEŃ PRZETSRZEGANIA POLITYKI… 26

II. INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI……..….. 27

1. NADAWANIE/ MODYFIKACJA/ ODBIERANIE UPRAWNIEŃ W SYSTEMACH INFORMATYCZNYCH……...….. 27

2. WYMOGI DOTYCZĄCE UŻYTKOWANIA KOMPUTERÓW PRZENOŚNYCH……. 29

3. STOSOWANE METODY I ŚRODKI UWIERZYTELNIANIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM……. 30

4. PROCEDURY ROZPOCZĘCIA, ZAWIESZANIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU…… 31

5. PROCEDURY TWORZENIA KOPII ZAPASOWYCH…… 32

6. SPOSÓB ZABEZPIECZENIANIA SYSTEMU INFORMATYCZNEGO ZMSP PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU……... 33

7. PRZEGLĄD I KONSERWACJA SYSTEMÓW INFORMATYCZNYCH…... 34

ZAŁĄCZNIK NR 1 WNIOSEK O NADANIE/ ZMIANĘ UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH……. 38

ZAŁĄCZNIK NR 2 OŚWIADCZENIE…….. 40

ZAŁĄCZNIK NR 3 WYKAZ POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ TWORZĄCY OBSZARY PRZETWARZANIA DANYCH OSOBOWYCH……... 41

Dział I

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA I OCHRONY DANYCH OSOBOWYCH

Rozdział 1

POSTANOWIENIA OGÓLNE

§ 1

1. Niniejszy dokument zatytułowany Polityka bezpieczeństwa przetwarzania i ochrony danych osobowych, zwany dalej jako „Polityka" ma za zadanie stanowić mapę wymogów i regulacji ochrony danych osobowych w Zarządzie Mienia Skarbu z siedzibą w Warszawie, ul. Prota 69, reprezentowanych przez Dyrektora Zarządu Mienia Skarbu Państwa, zwanego dalej jako „Administratorem".
2. Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawę swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych lub RODO) (Dz. Urz. UE L 119).
3. Polityka zawiera opis zasad ochrony danych osobowych obowiązujących w Zarządzie Mienia Skarbu Państwa i jest ona wiążąca dla wszystkich komórek organizacyjnych.
4. Z systemów przetwarzania danych osobowych znajdujących się w posiadaniu Administratora mogą korzystać również inne podmioty na podstawie odrębnych umów, porozumień lub stosunków prawnych, kształtowanych na podstawie przepisów szczególnych, określających zasady korzystania z tych systemów, w szczególności poprzez wyraźne zdefiniowanie celu i zakresu takiego korzystania oraz wskazanie odpowiedzialności karnej.

§ 2

1. Celem Polityki jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu ochrony i przetwarzania informacji zawierających dane osobowe.
2. Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, oprogramowanie użytkowe oraz użytkowników, proporcjonalne i adekwatne do ryzyka naruszenia bezpieczeństwa danych osobowych, przetwarzanych w ramach prowadzonej działalności.

3. Politykę stosuje się do ochrony podstawowych praw i wolności osób fizycznych, w szczególności ich prawa do ochrony danych osobowych przetwarzanych zarówno jednorazowo jak i wielokrotnie, w formie papierowej, elektronicznej oraz w systemach informatycznych, w sposób całkowicie lub częściowo zautomatyzowany.
4. Administratorem danych osobowych przetwarzanych w Zarządzie Mienia Skarbu Państwa jest Dyrektor.
5. Administrator wyznacza Inspektora Ochrony Danych na podstawie art. 37 RODO, w celu zapewnienia nadzoru nad przestrzeganiem zasad o przepisów ochrony danych osobowych.

Rozdział 2
DEFINICJE

§ 3

Użyte w Polityce określenia oznaczają:

1. Administrator – Dyrektor Zarządu Mienia Skarbu Państwa, który określa cele i sposoby przetwarzania danych osobowych.
2. Administrator Systemów Informatycznych (ASI) – pracownik wyznaczony przez Dyrektora Zarządu Mienia Skarbu Państwa, odpowiedzialny za sprawność, konserwację, wdrożenie i stosowanie zasad bezpieczeństwa danych w zakresie technicznych zabezpieczeń systemów informatycznych.
3. anominizacja - czynności uniemożliwiające ustalenie tożsamości osób, których dane osobowe dotyczą.
4. aplikacji – element oprogramowania użytkowego, jako program użytkowy, wyodrębniony ze względu na specjalistyczną funkcję, przygotowanych dla merytorycznych potrzeb danej komórki organizacyjnej.
5. autoryzacja – proces przyznawania osobie określonych upoważnień i uprawnień dostępu lub korzystania z zasobów danego programu, aplikacji lub innych zasobów wskazanego systemu informatycznego.
6. bezpieczeństwo przetwarzania danych osobowych – zachowanie poufności, integralności, dostępności i rozliczalności danych osobowych, ze szczególnym uwzględnieniem danych przetwarzanych w systemach informatycznych.
7. dane osobowe (dane) - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”), przy czym możliwa

do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

8. dane osobowe szczególnych kategorii – dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne dane biometryczne, przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby.
9. dane karne – dane dotyczące wyroków skazujących i naruszeń prawa.
10. incydent bezpieczeństwa - zdarzenie mogące wpłynąć na bezpieczeństwo danych osobowych w zakresie dostępności, poufności, integralności, może prowadzić do naruszenia ochrony danych osobowych.
11. komórka organizacyjna – komórka organizacyjna Zarządu Mienia Skarbu Państwa.
12. dostępność – właściwość zapewniająca, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, kiedy jest to potrzebne.
13. poufność – właściwość zapewniająca, że dane osobowe nie są udostępniane nieupoważnionym podmiotom (osobom).
14. integralność – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
15. rozliczalność – właściwość zapewniająca, że działania podmiotu (osoby) mogą być przypisane w sposób jednoznacznych tylko temu podmiotowi.
16. przetwarzanie danych – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
17. system informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych, zastosowanych w celu elektronicznego przetwarzania danych.

18. szyfrowanie – proces polegający na takim przetworzeniu informacji, aby nie mogły być one odczytane przez osoby nieupoważnione.
19. naruszenie ochrony danych osobowych – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
20. podmiot przetwarzający – osoba fizyczna, osoba prawna, organ publiczny, jednostka organizacyjna lub inny podmiot który przetwarza dane osobowe w imieniu Administratora.
21. państwo trzecie - państwo nie należące do Unii Europejskiej.
22. pracownik – osoba zatrudniona na podstawie umowy o pracę a także wolontariusz, stażysta lub praktykant.
23. pseudonimizacja – przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
24. rejestr czynności przetwarzania – prowadzony przez Administratora w formie pisemnej lub elektronicznej. zbiór informacji zawierający czynności przetwarzania.
25. rejestr kategorii czynności – rejestr prowadzony w formie pisemnej lub elektronicznej przez podmiot przetwarzający dla czynności przetwarzania zleconych przez Administratora.
26. udostępnianie danych – przekazywanie danych osobowych innemu administratorowi, które nie następuje w drodze umowy powierzenia przetwarzania, w wyniku udostępnienia podmiot, któremu przekazano dane osobowe staje się ich administratorem i samodzielnie decyduje o celach i sposobach przetwarzania.
27. usuwanie danych – zniszczenie danych lub taka ich nieodwracalna modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
28. użytkownik – osoba posiadająca upoważnienie od Administratora lub od osoby uprawnionej przez Administratora, uprawniona do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu.
29. zabezpieczenie systemu informatycznego – wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów

technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem lub pozyskaniem danych i ich ujawnieniem, a także utratą.

30. zgoda osoby której dane dotyczą – dobrowolne, konkretne, świadome i jednoznaczne oświadczenie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie.
31. Zarządzie (ZMSP) – Zarząd Mienia Skarbu Państwa.
32. Inspektorze Ochrony Danych (IOD) – osoba wyznaczona przez Administratora w celu wypełniania zadań określonych w art. 39 ust. 1 RODO.
33. zbiór danych – uporządkowany zestaw danych osobowych dostępny według określonych kryteriów niezależnie od tego czy zestaw tej jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
34. PUODO – Prezes Urzędu Ochrony Danych Osobowych.
35. Polityka - niniejsza Polityka Bezpieczeństwa Przetwarzania i Ochrony Danych Osobowych.

Rozdział 3
ZASADY OCHRONY DANYCH OSOBOWYCH

§ 4

Administrator tworzy system ochrony danych osobowych na podstawie:

a) podejścia opartego na ryzyku - polegającego na identyfikacji ryzyk związanych z przetwarzaniem danych osobowych oraz ustala operacje związane z danymi osobowymi;
b) poszanowania praw osób fizycznych - polegającego na realizacji praw osób, których dane dotyczą;
c) legalności - polegającej na zobowiązaniu Administratora oraz użytkowników do przeprowadzania operacji związanych z przetwarzaniem danych osobowych zgodnie z obowiązującym prawem;
d) bezpieczeństwa - polegającego na zobowiązaniu Administratora i użytkowników, że bezpieczeństwo przetwarzanych danych osobowych, uwzględnia stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz

ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze;

e) rozliczalności - polegającej na zobowiązaniu Administratora i użytkowników w zakresie dokumentowania operacji związanych z przetwarzaniem danych osobowych.

Rozdział 4
ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

§ 5

1. Dane osobowe w ZMSP przetwarza się zgodnie z prawem, wyłącznie da realizacji zadań wynikających z przepisów prawa, celów statutowych oraz regulaminowych. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach i w takim zakresie, jakim jest spełniony co najmniej jeden z poniższych warunków:
   a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
   b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba której dane dotyczą, lub podjęcia działań na żądanie osoby, której dane dotyczą przed zawarciem umowy;
   c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze;
   d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
   e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznych lub w ramach sparowania władzy publicznej powierzonej Administratorowi.
2. Przetwarzanie danych odbywa się:
   a) metodą klasyczną (papierową) w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych;
   b) w systemach informatycznych;
   c) w zbiorach danych lub poza zbiorami.

Rozdział 5

UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 6

1. Przetwarzanie danych osobowych w ZMSP możliwe jest wyłącznie przez osoby upoważnione przez Administratora, zgodnie z zakresem upoważnienia.
2. Administrator może upoważnić pracownika ZMSP, który w jego imieniu będzie realizował proces nadawania, zmiany i anulowania upoważnień do przetwarzania danych osobowych.
3. Upoważnienia do przetwarzania danych osobowych nadaje się:
   a) pracownikom ZMSP;
   b) wolontariuszom;
   c) stażystom;
   d) praktykantom;
   e) osobom realizującym na rzecz ZMSP usługi na podstawie umowy cywilnoprawnej, o ile jej realizacja związana jest z przetwarzaniem danych osobowych, zaś zapisy umowy nie określają w sposób wyczerpujący zasad dostępu do danych osobowych.
4. W przypadku umowy cywilnoprawnej zawierającej elementy powierzenia danych osobowych, osoby wskazane w umowie do jej realizacji przetwarzają dane osobowe na podstawie upoważnienia nadanego przez podmiot przetwarzający, któremu powierzono przetwarzanie ww. danych (Wykonawca), chyba że umowa powierzenia wiąże się z przetwarzaniem danych osobowych w systemie informatycznym ZMSP, wówczas upoważnienie wydawane jest przez Administratora.
5. Okres obowiązywania upoważnienia nie może być dłuższy niż okres związania umową lub okres realizacji usługi, o których mowa w ust. 2 i 3. W szczególnie uzasadnionych przypadkach, na wniosek kierownika komórki organizacyjnej ZMSP, Administrator może wyrazić zgodę na odstępstwo od tej zasady.
6. Upoważnienie nadawane jest na czas zatrudnienia w komórce organizacyjnej, pełnienia określonej funkcji lub na czas wykonywania czynności określonej w umowie cywilnoprawnej.
7. Upoważnienie traci moc w przypadku upływu terminu jego ważności oraz w sytuacji, gdy konieczna jest jego zmiana, w szczególności:
   a) rozwiązania umowy o pracę z użytkownikiem;
   b) zakończenia wykonywania funkcji przez użytkownika;
   c) zwolnienia pracownika z obowiązku świadczenia pracy;

d) zakończenia realizacji umowy cywilnoprawnej, w związku z którą zostało nadane, w szczególności w wyniku wypowiedzenia lub odstąpienia od umowy;
e) zakończenia stażu, praktyki, lub rozwiązania porozumienia dotyczącego wolontariatu;
f) w przypadku awansu na kierownicze stanowisko urzędnicze lub odwołania z niego.

8. Kierownicy komórek organizacyjnych ZMSP zobowiązani są do przekazywania informacji o których mowa w § 6 ust. 7 lit. a-f do komórki właściwej w sprawach ochrony danych osobowych.
9. Upoważnienie wymaga aktualizacji i zachowuje ważność do momentu wydania nowego w przypadku:
   a) zmiany imienia lub nazwiska użytkownika;
   b) zmiany nazwy komórki organizacyjnej, w której pracuje użytkownik.
10. Wnioski o nadanie/ zmianę upoważnienia do przetwarzania danych osobowych składane są przez kierowników komórek organizacyjnych ZMSP do komórki właściwej w sprawach ochrony danych osobowych. Wzór wniosku o nadanie/ zmianę upoważnienia do przetwarzania danych osobowych określa załącznik nr 1 do Polityki.
11. Warunkiem nadania upoważnienia jest złożenie przez pracownika pisemnego oświadczenia zawierającego jego zobowiązanie do przestrzegania obowiązujących przepisów z zakresu ochrony danych osobowych oraz do zachowania w tajemnicy wszelkich informacji dotyczących bezpieczeństwa danych osobowych, sposobów ich zabezpieczenia oraz zapewnienia bezpieczeństwa przetwarzania i ochrony danych osobowych w ZMSP. Wzór oświadczenia określa załącznik nr 2 do Polityki.
12. Oświadczenie zachowuje ważność przez cały okres zatrudnienia. Złożenie kolejnego oświadczenia jest wymagane w sytuacji zmiany imienia i nazwiska.
13. Wskazanie w umowie cywilnoprawnej, podczas realizacji której przetwarzane są dane osobowe, osób wyznaczonych do jej realizacji wiąże się z obowiązkiem podpisania przez nie oświadczenia, o którym mowa w ust. 11.
14. Oryginał oświadczenia przechowywany jest w komórce właściwej w sprawach ochrony danych osobowych.
15. Upoważnienia są nadawane, zmieniane i anulowane oraz ewidencjonowane przez komórkę właściwą w sprawach ochrony danych osobowych.
16. Egzemplarz upoważnienia przekazywany jest pracownikowi, o którym mowa w ust. 3 lit a, przez komórkę właściwą w sprawach ochrony danych osobowych.
17. Egzemplarz upoważnienia przekazywany jest użytkownikom, o których mowa w ust. 3 lit. b-e, przez kierownika komórki organizacyjnej.

Rozdział 6
ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

§ 7

1. Administrator przetwarza dane osobowe na podstawie zgody tylko wówczas, gdy nie ma innej podstawy przetwarzania danych osobowych. Nie należy uzyskiwać zgody na przetwarzanie danych osobowych, których obowiązek przetwarzania wynika z przepisów prawa lub jest związany z zawarciem i wykonaniem umowy.
2. Przed podjęciem decyzji o przetwarzaniu danych na podstawie zgody Administrator zobowiązany jest zweryfikować, czy dane osobowe są adekwatne do założonego celu przetwarzania.
3. Zgoda na przetwarzanie danych osobowych musi być udzielona świadomie i dobrowolnie, a jej uzyskanie poprzedzone realizacją obowiązku informacyjnego.
4. Zgody muszą być formułowane w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
5. Osoba, której dane dotyczą ma prawo do wycofania udzielonej zgody w każdym czasie. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.
6. Wycofanie zgody musi być równie łatwe jak i jej wyrażenie.

Rozdział 7
PRZETWARZANIE SZCZEGÓLNYCH KATEGORII DANYCH OSOBOWYCH

§ 8

1. W ZMSP przetwarzanie danych osobowych szczególnych kategorii jest możliwe wyłącznie, jeżeli osoba, której dane dotyczą wyraziła na to zgodę, a także w sytuacjach szczegółowo wskazanych w art. 9 RODO.
2. Podczas przetwarzania danych osobowych szczególnych kategorii należy zastosować zasady określone w art. 9 RODO.

Rozdział 8

PRZETWARZANIE DANYCH OSOBOWYCH DOTYCZĄCYCH WYROKÓW SKAZUJĄCYCH]

§ 9

W ZMSP są przetwarzane dane osobowe dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa.

Rozdział 9

MINIMALIZACJA

§ 10

1. W celu zapewnienia realizacji zasady minimalizacji danych osobowych w ZMSP podejmowane są przez Administratora następujące działania:
   a) weryfikacja ilości przetwarzanych danych osobowych w ZMSP nie można przetwarzać większej ilości danych osobowych niż to wynika z założonego celu;
   b) weryfikacja zakresu przetwarzanych danych osobowych w ZMSP nie może podejmować większej liczby czynności przetwarzania niż to wynika z założonego celu;
   c) ograniczanie dostępu do danych osobowych poprzez stosowanie środków prawnych – umowy z klauzulami poufności, upoważnienia do przetwarzania danych osobowych;
   d) ograniczanie dostępu do danych osobowych poprzez stosowanie środków fizycznych – kontrola dostępu osób do budynku, pomieszczeń, systemów informatycznych
   e) ograniczanie dostępu do danych osobowych poprzez stosowanie środków logicznych – kontrola uprawnień w systemach informatycznych, dostęp do systemów informatycznych.
   f) ograniczanie czasu przetwarzania danych osobowych, nie dłużej niż to wynika z założonego celu.

Rozdział 10

PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH

§ 11

W ZMSP przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych odbywa się zgodnie z postanowieniami rozdziału V RODO.

Rozdział 11

ZARZĄDZANIE RYZYKIEM

§ 12

1. Administrator wdraża i utrzymuje procedurę zarządzania ryzykiem.
2. Administrator zobowiązany jest uwzględnić ryzyko w planowanych i prowadzonych procesach przetwarzania danych osobowych.

Rozdział 12

OCENA SKUTKÓW DLA OCHRONY DANYCH

§ 13

1. W przypadkach wskazanych w art. 35 ust. 1 i 3 RODO Administrator przeprowadza ocenę skutków dla ochrony danych osobowych.
2. W odniesieniu do operacji przetwarzania danych w komunikacie publikowanym przez Prezesa Urzędu Ochrony Danych Osobowych na podstawie art. 35 ust. 4 RODO Administrator zobowiązany jest przeprowadzić ocenę skutków dla ochrony danych osobowych.
3. Jeżeli z oceny skutków dla ochrony danych osobowych wynika, że przetwarzanie powodowałoby wysokie ryzyko, gdyby Administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania Administrator jest zobowiązany skonsultować się z Prezesem Urzędu Ochrony Danych Osobowych.

Rozdział 13

ZASADY PRYWATNOŚCI W FAZIE PROJEKTOWANIA I W USTAWIENIACH DOMYŚLNYCH

§ 14

1. Administrator jest zobowiązany uwzględnić ochronę danych osobowych w fazie projektowania nowych systemów, programów, usług, a także w fazie projektowania nowych procesów i sposobów przetwarzania danych osobowych.
2. Administrator jest zobowiązany zapewnić domyślną ochronę danych osobowych domyślnie mogą być przetwarzane tylko te dane, które są niezbędne do osiągnięcia konkretnego celu przetwarzania. Rezygnacja z prywatności lub jej ograniczenie mogą nastąpić tylko na wyraźne żądanie podmiotu danych.

Rozdział 14
REJESTR CZYNNOŚCI PRZETWARZANIA

§ 15

1. W ZMSP prowadzony i aktualizowany jest rejestr czynności przetwarzania, który służy:
   a) inwentaryzowaniu i monitorowaniu sposobu przetwarzania danych osobowych;
   b) dokumentowaniu czynności przetwarzania;
   c) wykazaniu realizacji zasady rozliczalności.
2. Kierownicy komórek organizacyjnych ZMSP wykazują czynności przetwarzania do rejestru czynności przetwarzania oraz je przekazują do komórki właściwej w sprawach ochrony danych osobowych.

Rozdział 15
REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA

§ 16

1. W ZMSP prowadzony i aktualizowany jest rejestr kategorii czynności przetwarzania, który służy:
   a) inwentaryzowaniu i monitorowaniu sposobu przetwarzania danych osobowych w stosunku dla danych powierzonych;
   b) dokumentowania czynności przetwarzania;
   c) wykazaniu realizacji zasady rozliczalności.
2. Kierownicy komórek organizacyjnych ZMSP wykazują kategorie czynności przetwarzania do rejestru kategorii czynności przetwarzania oraz je przekazują do komórki właściwej w sprawach ochrony danych osobowych.

Rozdział 16
OBSZARY PRZETWARZANIA DANYCH OSOBOWYCH

§ 17

1. Za przetwarzanie danych uznaje się budynek, pomieszczenie lub część pomieszczenia, w którym przetwarzane są dane osobowe.
2. Przebywanie osób nieupoważnionych w obszarach przetwarzania danych w ZMSP jest ograniczone i może odbywać się tylko w obecności użytkowników upoważnionych,

od poniedziałku do piątku w godzinach 8.00-16.00. W innym przypadku niezbędne jest udzielenie na to indywidualnej zgody przez Administratora.

3. Przetwarzanie danych osobowych jest zabronione w pomieszczeniach, w których wykonywane są prace techniczne przez osoby nieupoważnione.
4. Monitory komputerów, na których przetwarzane są dane osobowe powinny być ustawione w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
5. Przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach.
6. Zabrania się pozostawiania dokumentów zawierających dane osobowe lub ich kopii, przy urządzeniach drukujących lub w innych miejscach dostępnych dla osób nieupoważnionych.
7. Po godzinach pracy ZMSP dokumenty papierowe, zawierające dane osobowe przechowuje się w zamykanych półkach i szafach (drewnianych oraz metalowych), a ich wynoszenie poza obszar przetwarzania może odbywać się wyłączeni za zgodą Administratora.
8. Użytkownicy obsługujący interesantów zobowiązani są do zachowania szczególnej uwagi w celu zabezpieczenia danych osobowych znajdujących się w ich posiadaniu.
9. W ramach działania ZMSP Administrator zapewnia całodobową ochronę obszarów przetwarzania danych osobowych.
10. Do obszarów podlegających szczególnej ochronie zalicza się:
    a) serwerownie i punkty dystrybucyjne;
    b) pomieszczenia, w których przechowywane są kopie zapasowe;
    c) Archiwum;
    d) pomieszczenia komórek organizacyjnych realizujących zadania związane z obsługą kadrową, płacową i finansową;
    e) obszary komórek organizacyjnych, w których realizowane są przedsięwzięcia związane z ewidencją ludności, gruntów i lokali.
11. Komórka właściwa w sprawach ochrony danych osobowych we współpracy z komórką właściwą w sprawach administracyjnych prowadzi Wykaz pomieszczeń lub części pomieszczeń tworzący obszary przetwarzania danych osobowych, zgodnie z tabelą, stanowiącą załącznik nr 3 do Polityki.

Rozdział 17

POWIERZENIE PRZETWARZANIA DANYCH ORAZ UDOSTĘPNIANIE

§ 18

1. Administrator może powierzyć przetwarzanie danych osobowych w swoim imieniu innemu podmiotowi, który zapewni wdrożenie odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi przepisów prawa i chroniło prawa osób, których dane dotyczą.
2. Powierzenie przetwarzania danych osobowych następuje w formie pisemnej umowy.
3. Przed powierzeniem przetwarzania danych osobowych innemu podmiotowi, kierownicy komórek organizacyjnych ZMSP, upewniają się czy stosowane przez ten podmiot środki techniczne i organizacyjne gwarantują bezpieczeństwo powierzonych danych.
4. W umowach powierzenia przetwarzania danych należy uwzględnić stosowne klauzule zapewniające bezpieczeństwo powierzonych danych.
5. W przypadku, gdy umowa nie wiąże się z przetwarzaniem danych osobowych, dla których Administratorem jest Dyrektor Zarządu Mienia Skarbu Państwa, należy wprowadzić stosowną klauzulę.
6. Komórka właściwa w sprawach ochrony danych osobowych prowadzi Rejestr zawartych umów powierzenia przetwarzania danych osobowych.
7. Dane osobowe mogą być udostępniane wyłącznie podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa oraz osobom, których dotyczą.
8. Udostępnianie danych osobowych może nastąpić wyłącznie za zgodą Administratora.
9. Informacje zawierające dane osobowe powinny być przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru listem poleconym za pokwitowaniem odbioru lub innym bezpiecznym sposobem, określonym wymogiem prawnym lub umową.
10. Udostępniając dane osobowe, należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

Rozdział 18

WSPÓŁADMINISTATORZY

§ 19

1. W przypadku, gdy w Zarządzie zachodzi sytuacja współadministrowania celami i sposobami przetwarzania danych przez Administratora i innego administratora lub administratorów, kierownicy komórek organizacyjnych zobowiązani

są do uzgodnienia zakresu swojej odpowiedzialności dotyczącej wypełnienia obowiązków wynikających z RODO, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw oraz wypełniania obowiązku informacyjnego.

2. Uzgodnienia, o których mowa w ust. 1, powinny odzwierciedlać zakresy obowiązków wszystkich współadministratorów oraz relacje pomiędzy nimi a osobami, których dane dotyczą. Zasadnicza treść uzgodnień jest udostępniona osobom, których dane dotyczą.
3. Osoba, której dane dotyczą może wykonywać przysługujące jej prawa wynikające z rozporządzenia RODO, wobec wszystkich współadministratorów.
4. Administrator zobowiązany jest zawrzeć z innym administratorem umowę o współadministrowanie danymi osobowymi. W umowie o współadministrowanie należy określić w szczególności:
   a) zakresy odpowiedzialności Administratora i innego administratora danych osobowych;
   b) sposób realizowania obowiązków wynikających z przepisów z zakresu ochrony danych osobowych;
   c) sposób spełnienia obowiązków informacyjnych zgodnie z art. 13 i 14 rozporządzenia RODO;
   d) punkt kontaktowy;
   e) relacje pomiędzy Administratorem i innym administratorem danych osobowych a osobami, których dane dotyczą;
   f) sposób przekazania podmiotom danych treści uzgodnień pomiędzy Administratorem a innym administratorem danych osobowych.

Rozdział 19
OBOWIĄZEK INFORMACYJNY

§ 20

1. Administrator jest zobowiązany realizować obowiązki informacyjne, o których mowa w art. 13 i 14 rozporządzenia RODO.
2. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, obowiązek informacyjny powinien być spełniany w momencie pozyskiwania danych osobowych.
3. W przypadku pozyskiwania danych osobowych w inny sposób, niż bezpośrednio od osoby, której dane dotyczą obowiązek informacyjny realizowany jest przez poszczególne komórki organizacyjne Zarządu:

a) w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
b) jeżeli dane osobowe mają być stosowane do komunikacji z osoba, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z tą osobą lub jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

Rozdział 20
ODPOWIEDZALNOŚĆ

§ 21

1. Za zgodne z prawem przetwarzania danych osobowych oraz ich ochronę w Zarządzie odpowiadają:
   a) Administrator;
   b) kierownicy komórek organizacyjnych;
   c) użytkownicy.
2. Do obowiązków Administratora należy:
   a) podejmowanie odpowiednich i niezbędnych środków technicznych i rozwiązań organizacyjnych dostosowanych do zagrożeń i kategorii przetwarzanych danych osobowych oraz ich aktualizacja;
   b) zapewnienie podstaw prawnych do przetwarzania danych osobowych w zakresie działania Urzędu od chwili zebrania danych osobowych do ich usunięcia;
   c) wyznaczenie Inspektora Ochrony Danych;
   d) udzielania upoważnień do przetwarzania danych osobowych;
   e) podział zadań i obowiązków związanych z organizacją ochrony danych osobowych;
   f) przekazywanie informacji o naruszeniu ochrony danych osobowych do Prezesa Urzędu Ochrony Danych Osobowych oraz prowadzenie postępowań wyjaśniających;
   g) decydowanie o przekazywaniu danych do państwa trzeciego;
   h) nadzorowanie przetwarzania danych osobowych w Zarządzie.
3. Do obowiązków kierowników komórek organizacyjnych należy:
   a) zapewnienie danym osobowym ochrony, zgodnie z zasadami określonymi w Polityce;
   b) realizacja obowiązku informacyjnego;

c) rozpatrywanie wniosków osób, których dane dotyczą, w zakresie przysługujących im praw oraz przekazywanie informacji do komórki właściwej w sprawach ochrony danych osobowych;
d) zgłaszanie do komórki właściwej w sprawach ochrony danych osobowych podejrzenia naruszenia zasad bezpieczeństwa i ochrony danych osobowych;
e) przekazywanie do komórki właściwej w sprawach ochrony danych osobowych informacji o czynnościach przetwarzania i ich aktualizacja w związku z prowadzonym Rejestrem Czynności Przetwarzania w Zarządzie;
f) przekazywania do komórki właściwej w sprawach ochrony danych osobowych informacji o kategoriach czynności przetwarzania i ich aktualizacja w związku z prowadzonym, Rejestrem Kategorii Czynności Przetwarzania w Zarządzie;
g) udzielanie wyjaśnień w toku postępowań administracyjnych prowadzonych Prezesa Urzędu Ochrony Danych Osobowych;
h) wnioskowania o nadanie/ zmianę upoważnienia do przetwarzania danych osobowych;
i) zgłaszania do Inspektora Ochrony Danych uwag dotyczących bezpieczeństwa przetwarzania i ochrony danych osobowych w Zarządzie;
j) wykonywania innych zadań wynikających z Polityki oraz dokumentów z nią związanych.

4. Do obowiązków użytkowników odpowiedzialnych za przetwarzanie danych osobowych należy znajomość i stosowanie dostępnych środków ochrony danych osobowych przed nieuprawnionym lub przypadkowym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem. Do obowiązków należy również:
a) posiadanie aktualnego upoważnienia do przetwarzania danych osobowych;
b) zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczania;
c) przetwarzania danych osobowych zgodnie z przepisami prawa, zapisami niniejszej Polityki oraz zakresem nadanego upoważnienia;
d) natychmiastowe zgłaszanie przełożonemu oraz komórce właściwej w sprawach ochrony danych osobowych incydentu związanego z bezpieczeństwem danych osobowych.

5. Do obowiązków komórki właściwej w sprawach ochrony danych osobowych należy w szczególności:
a) prowadzenie dokumentacji dotyczącej bezpieczeństwa i ochrony danych osobowych – ewidencji osób upoważnionych do przetwarzania danych osobowych;
b) wykazu obszarów przetwarzania danych osobowych;

c) Rejestru Czynności Przetwarzania;
d) Rejestru Kategorii Czynności Przetwarzania;
e) Rejestru udostępnień;
f) Rejestru umów powierzenia przetwarzania danych;
g) Rejestru incydentów bezpieczeństwa danych osobowych, w tym naruszeń ochrony danych osobowych oraz wszelkiej dokumentacji w tym zakresie;
h) Rejestru wniosków osób, których dane dotyczą;
i) opracowywanie dokumentacji dotyczącej przetwarzania danych osobowych, w tym uzgodnień umów, porozumień w zakresie ochrony danych osobowych.

6. Do obowiązków Inspektora Ochrony Danych należy w szczególności:
a) informowanie Administratora, kierowników komórek organizacyjnych ZMSP, użytkowników o spoczywających na nich obowiązkach, wynikających z przepisów prawa, Polityki i innych powiązanych dokumentów dotyczących ochrony danych osobowych;
b) weryfikacja stosowania w Zarządzie przepisów prawa obowiązujących w zakresie ochrony danych osobowych oraz Polityki, poprzez prowadzenie planowych i doraźnych kontroli przetwarzania i ochrony danych osobowych oraz nadzór nad realizacją działań naprawczych;
c) wskazywania w przypadkach spornych osób odpowiedzialnych za prawidłowe stosowanie przepisów dotyczących ochrony danych osobowych oraz Polityki;
d) współpraca z Prezesem Urzędu Ochrony Danych Osobowych w zakresie ochrony danych osobowych.

Rozdział 21
REALIZACJA ŻĄDAŃ OSÓB, KTÓRYCH DANE DOTYCZĄ

§ 22

1. Na wniosek osoby, której dane dotyczą, kierownicy komórek organizacyjnych ZMSP zobowiązani są do zapewnienia możliwości zrealizowania przysługujących jej praw, a w szczególności prawa do:
a) dostępu do przetwarzanych danych osobowych;
b) sprostowania danych osobowych;
c) uzasadnionego okolicznościami usunięcia dotyczących jej danych osobowych;

d) uzasadnionego okolicznościami żądania ograniczenia przetwarzania jej danych osobowych;
e) uzasadnionego okolicznościami żądania przeniesienia danych osobowych do innego administratora;
f) wniesienia sprzeciwu do przetwarzania jej danych osobowych;
g) niepodlegania automatycznemu profilowaniu jej danych.

2. Komórka właściwa w sprawach ochrony danych osobowych prowadzi Rejestr wniosków osób, których dane dotyczą.

Rozdział 22
POSTĘPOWANIE W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

§ 23

1. Za naruszenie ochrony danych osobowych uważa się w szczególności:
a) udostępnienie lub umożliwienie udostępnienia (przekazania) danych osobowych osobom lub podmiotom do tego nieupoważnionym;
b) zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia danym osobowym bezpieczeństwa i ochrony;
c) przetwarzanie danych osobowych bez aktualnego upoważnienia lub niezgodne z jego zakresem;
d) niedopełnienie obowiązku zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczania;
e) kradzież danych;
f) przetwarzanie danych osobowych niezgodnie z celem ich przetwarzania;
g) przetwarzanie danych osobowych szczególnych, gdy ich przetwarzanie nie jest dopuszczalne;
h) naruszenie praw osób, których dane osobowe są przetwarzane;
i) nieuprawniony dostęp do obszarów, w których przetwarzane są dane osobowe;
j) naruszenie zasad bezpieczeństwa w systemie informatycznym wykorzystywanym do przetwarzania danych osobowych;
k) przetwarzanie danych w systemie przez osoby nieuprawnione;

l) kradzież lub zniszczenie urządzeń, wszelkie działanie uniemożliwiające prawidłowe funkcjonowanie systemu, niszczenie elektronicznych nośników informacji lub ich kopii służących do przetwarzania danych osobowych;

m) przesyłanie przez użytkowników w sieci publicznej informacji zawierających dane osobowe bez zapewnienia im cech: poufności, rozliczalności i integralności;

n) nieautoryzowane wejście do systemu lub nieautoryzowaną modyfikację danych osobowych w systemie informatycznym;

o) ujawnienie lub udostępnienie innym osobom lub użytkownikom hasła dostępu do systemu;

p) korzystanie z haseł, identyfikatorów lub uprawnień innych użytkowników;

q) wykorzystywanie urządzeń oraz programów zagrażających bezpieczeństwu ochrony danych osobowych;

r) inne działania lub zaniechania zagrażające bezpieczeństwu przetwarzania i ochrony danych osobowych w systemie informatycznym.

2. Każdy użytkownik, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych, zobowiązany jest do niezwłocznego poinformowania o zaistniałym zdarzeniu swojego przełożonego oraz komórkę właściwą w sprawach ochrony danych osobowych, w formie elektronicznej na adres mailowy incydenty@zmsp.warszawa.pl albo w formie elektronicznej i papierowej.

3. W przypadku braku możliwości skorzystania z formy elektronicznej albo elektronicznej i papierowej informacje, o których mowa w ust. 1, należy przekazać w każdej dostępnej formie, zapewniającej dotarcie informacji o naruszeniu, do osób wskazanych w ust. 2.

4. Kierownicy komórek organizacyjnych mają obowiązek niezwłocznego, nie później niż w ciągu 12 godzin od stwierdzenia naruszenia, przekazania komórce właściwej w sprawach ochrony danych osobowych, informacji o okolicznościach zdarzenia. W szczególności zobowiązani są:

a) opisać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazać kategorie i przybliżoną liczbę osób, których dane dotyczą oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

b) opisać możliwe konsekwencje naruszenia ochrony danych osobowych i środki zastosowane lub proponowane w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach - środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

5. Za nieprzestrzeganie obowiązku, określonego w ust. 2, grozi odpowiedzialność służbowa.
6. W przypadku naruszenia ochrony danych osobowych powodującego wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator lub osoba przez niego upoważniona niezwłocznie, nie później niż w ciągu 72 godz. po stwierdzeniu naruszenia - informuje organ nadzorczy o zaistniałym fakcie.
7. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator niezwłocznie zawiadamia o tym fakcie osoby, których dane dotyczą.

Rozdział 23
ŚRODKI OCHRONY DANYCH

§ 24

1. Przez bezpieczeństwo przetwarzanych danych osobowych w ZMSP należy rozumieć zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie.
2. Poziom bezpieczeństwa jest mierzony akceptowalną wielkością ryzyka związanego z ochroną danych osobowych.
3. Zastosowane zabezpieczenia mają zapewnić:
   a) poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
   b) integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   c) rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
   d) integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
   e) dostępność informacji – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
   f) zarządzanie ryzykiem – rozumiane jako identyfikowanie podatności i zagrożeń oraz szacowanie ich prawdopodobieństwa wystąpienia i siły oddziaływania (skutków), identyfikowanie istniejących zabezpieczeń oraz wdrażanie wymaganych zabezpieczeń, opracowanie planu postępowania z ryzykiem nieakceptowalnym (wysokim w rozumieniu RODO), monitorowanie skuteczności stosowanych środków

organizacyjnych, technicznych i kadrowych mających zapewnić bezpieczeństwo przetwarzania danych osobowych.

4. Administrator zapewnia bezpieczeństwo danych, poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, oprogramowanie użytkowe oraz należyte przygotowanie użytkowników, proporcjonalne i adekwatne do ryzyka naruszenia bezpieczeństwa i ochrony danych osobowych przetwarzanych w zakresie realizacji zadań Zarządu.
5. Podczas projektowania nowych systemów, projektów, inwestycji i rozwiązań organizacyjnych, w zakresie, jakim dotyczą one przetwarzania danych osobowych, kierownicy komórek organizacyjnych powinni uwzględniać ich wpływ na ochronę praw osób fizycznych, których dane dotyczą.
6. Do środków ochrony fizycznej zalicza się w szczególności:
   a) lokalizację miejsc przetwarzania danych osobowych w pomieszczeniach o ograniczonym i kontrolowanym dostępie;
   b) wdrożenie i nadzorowanie zasad gospodarki kluczami w Zarządzie;
   c) wyposażenie obszarów przetwarzania danych osobowych w Zarządzie w sposób gwarantujący bezpieczeństwo przetwarzania i ochrony danych osobowych, odpowiedni do kategorii przetwarzanych danych osobowych.
7. Do środków ochrony organizacyjnej zalicza się w szczególności:
   a) opracowanie i wdrożenie Polityki, Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, a także ich stałą aktualizację;
   b) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
   c) umożliwienie przetwarzania danych osobowych wyłącznie osobom posiadającym upoważnienie;
   d) przeprowadzanie stosownych szkoleń z zakresu przepisów dotyczących bezpieczeństwa przetwarzania i ochrony danych osobowych;
   e) składanie oświadczeń o zachowaniu w tajemnicy danych osobowych i sposobów ich zabezpieczenia oraz zapoznania się z zasadami przetwarzania danych osobowych;
   f) stosowanie pisemnych umów powierzenia przetwarzania danych osobowych;
   g) szacowanie ryzyka zagrożeń przetwarzania danych osobowych dla Zarządu oraz osób fizycznych;
   h) zapewnienie dostępności i odporności systemów i usług przetwarzania;
   i) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich, w razie incydentu fizycznego lub technicznego;

j) nadzór nad przestrzeganiem przez użytkowników i inne osoby przetwarzające dane w imieniu Administratora zasad określonych w Polityce;
k) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych;
l) pseudonimizację i szyfrowanie danych osobowych;
m) inne działania, których celem jest realizacja zasad bezpieczeństwa przetwarzania i ochrony danych osobowych w Zarządzie.

8. Środki ochrony technicznej obejmują zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej oraz zabezpieczenia narzędzi programowych i baz danych. Zabezpieczenia stosuje się dla fizycznych elementów systemu, ich połączeń oraz systemów operacyjnych.
9. Szczegółowy opis zabezpieczeń technicznych określa Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.

Rozdział 24
MONITOROWANIE PRZESTRZEGANIA POSTANOWIEŃ POLITYKI

§ 25

1. Przynajmniej raz na rok Administrator w porozumieniu z Inspektorem Ochrony Danych dokonuje przeglądu niniejszej Polityki oraz załączników.
2. Niniejsza Polityka wraz z załącznikami jest aktualizowana, rozwijana i modyfikowana:
   a) na potrzeby dostosowania do zmiany stanu prawnego;
   b) na potrzeby zwiększenia jej skuteczności;
   c) w związku z potrzebami Administratora.
3. Administrator jest zobowiązany podejmować działania na rzecz zwiększenia świadomości z zakresu ochrony danych osobowych wśród użytkowników oraz podnoszenia ich wiedzy i kwalifikacji w tym zakresie.
4. Przynajmniej raz na dwa lata Inspektor Ochrony Danych przeprowadza audyt w zakresie przestrzegania ochrony danych osobowych w zakresie:
   a) ilości przetwarzania danych osobowych;
   b) procesów przetwarzania danych osobowych;
   c) upoważnień do przewarzania danych osobowych;
   d) użytkowników w systemach informatycznych.

5. W zakresie wynikającym z audytu dokonuje się niezbędnych usunięć, aktualizacji aby zapewnić zgodność z niniejszą Polityką.

Dział II

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI

Rozdział 1

NADAWANIE/ MODYFIKACJA/ ODBIERANIE UPRAWNIEŃ W SYSTEMACH INFORMATYCZNYCH

§ 26

Aby dana osoba była zarejestrowana w systemie informatycznym, jako użytkownik, muszą być spełnione następujące warunki:

a) złożenie oświadczenia o znajomości RODO oraz innych przepisów prawnych dotyczących ochrony danych osobowych;
b) złożenie oświadczenia o znajomości Polityki;
c) uzyskanie od Administratora imiennego upoważnienia do przetwarzania danych osobowych w zakresie działania Zarządu;
d) dostęp do systemów informatycznych stosowanych w ZMSP, w których są przetwarzane dane osobowe, nadawany jest na podstawie wniosku, którego wzór zawarty jest w załączniku nr 1 do Polityki, podpisanego przez kierownika komórki organizacyjnej, której ma zostać nadane lub inną osobę upoważnioną w danej komórce organizacyjnej.

§ 27

Pracowników ZMSP w systemach, o których mowa w § 26, rejestrują pracownicy wydziału właściwego w sprawach informatycznych, po uwierzytelnieniu informacji zawartych we wniosku. Wnioskodawcy otrzymują informację o dacie nadania uprawnień i zakresie uprawnień użytkownika w systemach.

§ 28

Stosowne uprawnienia użytkownika w systemach określa we wniosku kierownik komórki organizacyjnej lub osoba przez niego upoważniona, uwzględniając zadania wynikające z zajmowanego przez pracownika stanowiska.

§ 29

Zmiana uprawnień użytkownika w systemach dokonywana jest przez pracowników wydziału właściwego w sprawach informatycznych i może obejmować:

a) zmianę uprawnień użytkownika;
b) zmniejszenie, odebranie lub zawieszenie dotychczas posiadanych uprawnień użytkownika (ograniczenie uprawnień).

§ 30

1. Ograniczenie uprawnień, o którym mowa w § 29 lit. b, następuje w momencie:
   a) utraty ważności upoważnienia do przetwarzania danych osobowych;
   b) na wniosek Administratora;
   c) na wniosek przełożonego upoważnionego;
   d) na wniosek IOD.
2. W przypadku zawieszenia dotychczas posiadanych uprawnień, o którym mowa w § 29 lit. b, ponowne nadanie uprawnień wymaga realizacji postanowień, o których mowa w § 28.

§ 31

1. Użytkownik jest wyrejestrowywany z systemu informatycznego po utracie przez niego uprawnień do dostępu do danych osobowych, co ma miejsce w szczególności, w następujących przypadkach:
   a) ustanie stosunku pracy;
   b) zmiana zakresu obowiązków;
   c) wniosek Kierownika jednostki;
   d) w nadzwyczajnych przypadkach, kiedy zachodzi zagrożenie ochrony danych osobowych stwierdzone przez pracownika komórki właściwej w sprawach informatycznych.
2. Uprawnienia są odbierane po przekazaniu stosownej informacji do pracownika komórki właściwej w sprawach informatycznych:
   a) od komórki organizacyjnej właściwej w sprawach kadrowych - w takiej sytuacji dostęp do systemów jest usuwany najpóźniej do ostatniego dnia miesiąca, w którym kończy się zatrudnienie danego pracownika lub na wniosek;
   b) od przełożonego pracownika upoważnionego - w takiej sytuacji dostęp do systemów jest blokowany niezwłocznie.

3. Pracownik komórki właściwej w sprawach informatycznych przekazuje kierownikowi komórki organizacyjnej pracownika informacje o odebraniu uprawnień oraz informuje właściwą komórkę właściwą w sprawach ochrony danych osobowych.

Rozdział 2
WYMOGI DOTYCZĄCE UŻYTKOWANIA KOMPUTERÓW PRZENOŚNYCH

§ 32

1. Użytkownicy, którym zostały powierzone komputery przenośne, powinni chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych.
2. Zaleca się szczególną ostrożność podczas transportu komputerów przenośnych, a w szczególności stosowanie się do poniższych zasad:
   a) nie wolno pozostawiać komputera przenośnego bez dozoru;
   b) zabronione jest pozostawianie komputera przenośnego w zaparkowanym samochodzie, nawet jeżeli jest on umieszczony w zamkniętym bagażniku;
   c) komputer przenośny należy przewozić albo w zamkniętym bagażniku albo na podłodze w miejscu przeznaczonym na nogi pasażera, nie wolno przewozić komputera przenośnego na tylnym siedzeniu.
3. Zabronione jest odstępowanie komputera przenośnego osobom trzecim.
4. Obowiązuje zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone.
5. Praca na komputerze przenośnym możliwa jest po wprowadzeniu hasła i indywidualnego identyfikatora użytkownika.
6. Użytkownicy są zobowiązani zmieniać hasła w komputerach przenośnych nie rzadziej niż raz na 30 dni.
7. Komputery przenośne posiadają dodatkowe zabezpieczenie w postaci zaszyfrowanych dysków twardych. Za szyfrowanie, o którym mowa odpowiada komórka właściwa w sprawach informatycznych.
8. Komputer przenośny ma służyć pracownikowi tylko i wyłącznie do wspomagania jego zadań w ramach wykonywanych obowiązków.
9. W razie wystąpienia usterek w pracy komputerów przenośnych lub w razie wystąpienia konieczności aktualizacji ich oprogramowania należy zgłosić to ASI.
10. Ochrona sprzętu w przypadku próby kradzieży powinna być adekwatna do zagrożenia, tzn. nie może powodować zagrożenia życia lub zdrowia użytkownika.

11. Komputery przenośne wyposażone są w aktualnie stosowany i na bieżąco aktualizowany programy ochrony antywirusowej.

Rozdział 3
STOSOWANE METODY I ŚRODKI UWIERZYTELNIANIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

§ 35

1. W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się system uwierzytelniania na poziomie dostępu do systemu operacyjnego i aplikacji oraz, jeśli jest taka potrzeba, do serwera.
2. Do uwierzytelnienia użytkownika w systemie informatycznym bezwzględnie stosuje się identyfikatory i hasła.
3. Niedopuszczalne jest korzystanie z tego samego identyfikatora przez więcej niż jednego użytkownika.
4. Raz użyty identyfikator nie powinien być przydzielany innemu użytkownikowi.
5. Identyfikator oraz pierwsze hasło (tymczasowe) przekazywane są użytkownikowi przez pracownika wydziału właściwego w sprawach informatycznych.
6. Hasła przekazywane są bezpośrednio użytkownikowi.
7. Przy pierwszym logowaniu użytkownik zmienia hasło tymczasowe na własne i rejestruje je w systemie.
8. Hasło dostępu składa się, co najmniej z 8 znaków i zawiera małe i wielkie litery oraz cyfry lub znaki specjalne. W przypadku aplikacji niespełniających powyższego wymogu stosuje się najdłuższe możliwe hasło (uwzględniające małe i wielkie litery, cyfry lub znaki specjalne).
9. Hasła nie powinny być powszechnie używanymi słowami, w szczególności nie należy, jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów, itp.
10. Hasła w ZMSP podlegają okresowej (raz na 30 dni) zmianie wymuszanej przez system.
11. Należy unikać stosowania tego samego hasła do ochrony różnych zasobów, np. to samo hasło do systemu operacyjnego, aplikacji i poczty elektronicznej.
12. W przypadku podejmowania kilku kolejnych nieudanych prób uwierzytelnienia do systemu informatycznego, system ten powinien automatycznie blokować się, a jego

odblokowania dokonuje pracownik wydziału zajmującego się sprawami informatycznymi.

13. Hasła wpisywane z klawiatury nie mogą pojawiać się na ekranie monitora w formie jawnej.
14. Hasło nie może być ujawnione osobom nieupoważnionym nawet po utracie przez nie ważności.
15. W przypadku podejrzenia, że hasło mogła poznać osoba nieupoważniona, użytkownik zobowiązany jest do jego natychmiastowej zmiany.
16. Zabrania się zapisywania haseł, a w szczególności przechowywania ich w miejscach, w których mogą się z nimi zapoznać osoby postronne.

Rozdział 4
PROCEDURY ROZPOCZĘCIA, ZAWIESZANIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU

§ 36

1. Użytkownik w czasie pracy powinien przedsięwziąć wszelkie czynności zapewniające bezpieczeństwo przetwarzania danych osobowych, a w szczególności:
   a) ekran monitora ustawić tak, aby uniemożliwić wgląd w przetwarzane dane osób nieuprawnionych;
   b) dopilnować, aby w pomieszczeniach, gdzie przetwarzane są dane osobowe, osoby trzecie przebywały tylko w obecności osób uprawnionych.
2. W ramach procedury rozpoczęcia pracy w systemie pracownik powinien:
   a) uruchomić komputer i zalogować się podając swój identyfikator i hasło dostępu do systemu operacyjnego;
   b) uruchomić aplikację, wpisując swój identyfikator i hasło dostępu;
   c) rozpocząć pracę.
3. Przy każdorazowym opuszczeniu stanowiska komputerowego należy dopilnować, aby na ekranie nie były wyświetlane dane osobowe.
4. Przed opuszczaniem miejsca pracy na dłuższy czas użytkownik obowiązany jest zablokować komputer do ekranu logowania hasłem lub wylogować się z systemu.
5. W ramach procedury zakończenia pracy w systemie pracownik powinien:
   a) wylogować się z aplikacji i zamknąć aplikację;
   b) zamknąć system.

Rozdział 5
PROCEDURY TWORZENIA KOPII ZAPASOWYCH

§ 37

1. W ZMSP tworzone są kopie bezpieczeństwa systemów oraz programów i narzędzi programowych zabezpieczające dane osobowe.
2. Kopie zapasowe obejmują wszystkie dane zawarte systemie.
3. Kopie bezpieczeństwa zapisywane są na serwerach znajdujących się w serwerowni jak także na wymiennych nośnikach danych, dopuszczonych do użytku przez IOD.
4. ASI tworzy kopie dzienne, tygodniowe oraz miesięczne.
5. Nośnik elektroniczny może być wykorzystywany do wielokrotnego zapisu.
6. Po wycofaniu nośnika wykorzystywanego do zapisu na skutek utraty przydatności lub uszkodzenia nośnik pozbawia się wszelkich danych osobowych poprzez kasowanie nie odtwarzalne lub fizyczne zniszczenie nośnika.
7. O konieczności odtworzenia danych systemu decyduje Administrator w porozumieniu z IOD.

§ 38

1. Dane osobowe przetwarzane w systemie informatycznym ZMSP przechowywane są na serwerach znajdujących się w serwerowni zlokalizowanej w siedzibie ZMSP.
2. Przechowywanie danych osobowych na nośnikach przenośnych innych niż nośniki kopii zapasowych dozwolone jest wyłącznie w uzasadnionych przypadkach, za wiedzą i zgodą IOD.
3. W zależności od rodzaju i przeznaczenia danych IOD każdorazowo określa miejsce i okres przechowywania nośnika.
4. Nieuprawnione tworzenie kopii danych osobowych na wymiennych nośnikach jest niedozwolone.
5. Dane osobowe przechowywane są przez czas niezbędny dla spełnienia celu, dla którego są one przetwarzane, po jego upływie dane podlegają usunięciu poprzez kasowanie nie odtwarzalne lub zniszczenie nośnika.
6. W przypadku wycofania sprzętu komputerowego z użycia dane osobowe na nim zapisane są niszczone poprzez kasowanie nie odtwarzalne lub zniszczenie nośnika. Za usunięcie danych odpowiada ASI.

7. Nośniki zawierające kopie zapasowe przechowuje się w szafie pancernej w pomieszczeniu wskazanym przez IOD, innym niż serwerownia, w której znajduje się środowisko produkcyjne. Dostęp do szafy pancernej posiadają: Administrator, IOD, ASI oraz upoważnione osoby.

§ 39

1. W celu weryfikacji możliwości przywracania danych z kopii zapasowych wykonywane są testy przywracania danych.
2. Testy wykonuje ASI nie rzadziej niż raz na sześć miesięcy sporządzając dokumentacje z przeprowadzonych prac.
3. Testy obejmują wybrane systemy operacyjne oraz przechowywane dane.

Rozdział 6

SPOSÓB ZABEZPIECZENIANIA SYSTEMU INFORMATYCZNEGO ZMSP PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU

§ 40

Drogą umożliwiającą przedostanie się wirusów lub innego szkodliwego oprogramowania może być sieć publiczna, wewnętrzna sieć teleinformatyczna lub nośniki informacji elektronicznej.

§ 41

1. Czynności związane z ochroną antywirusową wykonuje ASI.
2. Ochronę antywirusową zapewnia program antywirusowy zainstalowany na każdym komputerze stacjonarnym lub przenośnym.
3. Oprogramowanie antywirusowe jest uaktualniane automatycznie (minimum raz na 24 godziny) bez konieczności interwencji użytkownika.
4. ASI zobowiązany jest do okresowej (nie rzadziej niż raz na kwartał) kontroli antywirusowej systemów informatycznych, natomiast sam program antywirusowy powinien mieć aktywny skaner wykrywający na bieżąco wszelkie zagrożenia.

§ 42

1. Użytkownicy mają zakaz używania nośników pochodzących z nieznanych źródeł lub z systemów o niższym stopniu zabezpieczenia antywirusowego bez uprzedniego sprawdzenia tych nośników za pomocą aktualnego programu antywirusowego.
2. Ochronę przed nieautoryzowanym dostępem do sieci zapewnia firewall.
3. Użytkownik jest obowiązany zawiadomić ASI o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.
4. ASI sprawdza typ zagrożenia powodowanego przez wirus oraz usuwa go z dysku twardego lub innych nośników.
5. Każdy przypadek wykrycia wirusa jest odnotowany w Rejestrze Incydentów Bezpieczeństwa przechowywanym w formie elektronicznej.

§ 43

Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym ZMSP, system ten zapewnia odnotowanie:

a) daty pierwszego wprowadzenia danych do systemu;
b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu;
c) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
d) informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia.

Rozdział 7
PRZEGLĄD I KONSERWACJA SYSTEMÓW INFORMATYCZNYCH

§ 44

1. Za wykonywanie przeglądów i konserwację systemów odpowiedzialny jest ASI.
2. Nieprawidłowości ujawnione w trakcie działań związanych z przeglądami i konserwacją zostaną niezwłocznie usunięte, a ich przyczyny będą przeanalizowane i przekazane IOD.

§ 45

1. Przegląd systemu polega w szczególności na sprawdzeniu jego konfiguracji oraz sprawdzeniu logów systemowych.
2. Przeglądu systemu dokonuje się raz w miesiącu oraz doraźnie w sytuacjach wystąpienia incydentów mogących mieć wpływ na bezpieczeństwo danych osobowych.

3. W przypadku stwierdzenia nieprawidłowości w systemie, ASI usuwa je, wykorzystując dostępne narzędzia.
4. Na przegląd systemu składają się następujące zadania:
   a) sprawdzenie dostępu do zbiorów/ zestawów danych na poziomie użytkowników o różnych prawach dostępu i ich wyrywkowa weryfikacja;
   b) w przypadku stwierdzenia nieprawidłowości w stanie zbiorów/ zestawów danych lub naruszenia praw dostępu, ASI powiadamia o zaistniałym fakcie IOD, a następnie podejmuje działania zmierzające do usunięcia nieprawidłowości i zidentyfikowania osoby, która doprowadziła do ich powstania.
5. Na sprawdzenie poprawności działania programów składają się następujące czynności:
   a) sprawdzanie poprawności działania programów rozumiane jako sprawdzenie poprawności zalogowania się do systemu, poprawności zalogowania się do aplikacji, sprawdzenia funkcjonowania logów, przeprowadza się w szczególności w następujących sytuacjach:
      - zmiana wersji i aktualizacja oprogramowania stanowiska komputerowego użytkownika systemu;
      - zmiana systemu operacyjnego stanowiska komputerowego użytkownika systemu;
   b) wykonanie zmian w projekcie systemu spowodowanych koniecznością naprawy, konserwacji lub modyfikacji systemu.
6. Konserwacja oprogramowania rozumiana jako sprawdzenie poprawności działania oraz wgrania ewentualnych aktualizacji przeprowadza się po zgłoszeniu przez użytkownika systemu takiej potrzeby. Konserwację przeprowadza ASI.

§ 46

1. W przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych w systemie informatycznym tworzony jest zespół obejmujący IOD, ASI oraz bezpośredniego przełożonego użytkownika, który zgłosił naruszenie, o którym mowa.
2. Użytkownik zobowiązany jest zawiadomić bezpośredniego przełożonego o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu, a w szczególności o:
   a) naruszeniu hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź też można przetwarzać dane bez wprowadzenia hasła);
   b) częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień;

c) braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera;
d) wykryciu wirusa komputerowego;
e) zauważeniu elektronicznych śladów próby włamania do systemu informatycznego;
f) podejrzeniu kradzieży sprzętu komputerowego, nośników lub dokumentów zawierających dane osobowe;
g) zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf;
h) stwierdzeniu nielegalnego ujawnienia danych osobowych osobom nieupoważnionym.

3. Informacje, o których mowa w ust. 2, bezpośredni przełożony pracownika przekazuje IOD i ASI.
4. Do czasu podjęcia interwencji przez jednego z członków zespołu, użytkownik (bezpośredni przełożony, ASI lub IOD) powinien:
   a) o ile istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego zdarzenia, a następnie uwzględnić w działaniu również ustalenie jego przyczyn lub sprawców;
   b) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę.
5. Członek zespołu po otrzymaniu zawiadomienia, o którym mowa wyżej powinien niezwłocznie:
   a) przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia ochrony danych osobowych;
   b) podjąć działania chroniące system przed ponownym naruszeniem;
   c) w przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu sporządzić raport naruszenia bezpieczeństwa systemu informatycznego Administratora, a następnie niezwłocznie przekazać jego kopię Administratorowi;
6. Raport, o którym mowa w ust. 5 lit. c, powinien zawierać w szczególności:
   a) opis naruszenia (czas i datę, miejsce, okoliczności, inne istotne informacje);
   b) opis działań, jakie zostały zrealizowane;
   c) stan systemu/urządzeń/pomieszczeń po zakończeniu działań awaryjnych;
   d) zalecenia mające na celu ograniczenie ponownego wystąpienia zagrożenia;
   e) oszacowanie strat i ryzyka związanego z bezpieczeństwem danych osobowych.
7. ASI może zarządzić, w razie potrzeby, odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części.

8. W razie odtwarzania danych z kopii zapasowych ASI obowiązany jest upewnić się, że odtwarzane dane zapisane zostały przed wystąpieniem incydentu.
9. Administrator po zapoznaniu się z raportem, o którym mowa w ust. 5 lit c, podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego Administratora bądź zastosowaniu środków ochrony fizycznej.

§ 47

ASI zobowiązany jest do informowania Administratora o awariach systemu informatycznego, zauważonych przypadkach naruszenia niniejszej Instrukcji przez użytkowników, a zwłaszcza o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami, nieprzestrzegania zasad używania oprogramowania antywirusowego, niewłaściwego wykorzystania sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z procedurami ochrony danych osobowych.

Załącznik nr 1
do Polityki bezpieczeństwa przetwarzania
i ochrony danych osobowych oraz
Instrukcji Zarządzania Systemami Informatycznymi

…….
(imię i nazwisko Wnioskującego)

……..
(stanowisko i nazwa komórki organizacyjnej)

Dyrektor
Zarządu Mienia
Skarbu Państwa

WNIOSEK
o nadanie/ zmianę upoważnienia do przetwarzania danych osobowych

na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), wnioskuję o nadanie upoważnienia do przetwarzania danych osobowych

dla

Pani/ Pana ……..……

Podstawa do nadania upoważnienia (np. umowa o pracę/ umowa cywilnoprawna). Przyczyna zmiany/ aktualizacji upoważnienia (np. zmiana nazwiska, zmiana komórki organizacyjnej).
…….
…….

Czas obowiązywania upoważnienia: …….

1. Uprawnieninia: z tytułu zajmowanego stanowiska/jakiego/:

   …….

2. Zakres przetwarzania danych (proszę zaznaczyć **X** wybrane elementy):

W przypadku zmiany upoważnienia proszę zaznaczyć wszystkie elementy po uwzględnieniu zmian.

□ SignUm □ konto ZMSP

□ dysk wydziałowy □ skrzynka pocztowa

□ Budżet – Księgowość Budżetowa □ UW - użytkowanie wieczyste

□ KSZOB – Księgowość zobowiązań □ Czynsze i media

□ Kadry - płace □ FK – Finanse i księgowość

□ Edok …… □ inne ……

3. Sposób przetwarzania danych osobowych: papierowy/informatyczny/*
4. Obszar przetwarzania danych osobowych /piętro i nr pokoju/: …….
5. Uprawnienia obejmują przetwarzanie danych szczególnych kategorii – art. 9 RODO/ danych */tak / nie
6. Uprawnienia obejmują przetwarzanie danych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa – art. 10 RODO */tak / nie

……..
Podpis wnioskującego

/* niepotrzebne proszę skreślić

Załącznik nr 2
do Polityki bezpieczeństwa przetwarzania
i ochrony danych osobowych oraz
Instrukcji Zarządzania Systemami Informatycznymi

.....
(imię i nazwisko)

.....
(stanowisko i nazwa komórki organizacyjnej/ nazwa podmiotu)

OŚWIADCZENIE

Ja, niżej podpisana(y), oświadczam, że zapoznała(e)m się z przepisami dotyczącymi przetwarzania i ochrony danych osobowych i zobowiązuję się do przestrzegania:

1. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz wydanymi na jego podstawie krajowymi przepisami z zakresu ochrony danych osobowych.

2. Zasad bezpieczeństwa przetwarzania i ochrony danych osobowych, określonych przez Administratora – Dyrektora Zarządu Mienia Skarbu Państwa.

<u>*Jednocześnie oświadczam, że:*</u>

a) Zachowam w tajemnicy wszelkie informacje dotyczące danych osobowych przetwarzanych w Zarządzie Mienia Skarbu Państwa oraz sposobów ich zabezpieczenia.

b) Zapewnię bezpieczeństwo i ochronę danym osobowym przetwarzanym w Zarządzie Mienia Skarbu Państwa, a w szczególności zabezpieczę je przed dostępem osób nieupoważnionych, zabraniem, uszkodzeniem oraz nieuprawnioną modyfikacją lub zniszczeniem.

c) Natychmiast zgłoszę przełożonemu lub w uzasadnionych przypadkach bezpośrednio Inspektorowi Ochrony Danych w Zarządzie Mienia Skarbu Państwa (IOD), stwierdzenie próby lub faktu naruszenia ochrony danych oraz zagrożenia ich bezpieczeństwa w systemach informatycznych.

…….....
(podpis osoby ubiegającej się o upoważnienie)

Warszawa, dnia ……

Załącznik nr 3

do Polityki bezpieczeństwa przetwarzania

i ochrony danych osobowych oraz

Instrukcji Zarządzania Systemami Informatycznymi

WYKAZ POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ TWORZĄCY OBSZARY PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Nazwa Wydziału	Nazwa ulicy i nr budynku:	Nr piętra [numery rzymskie] i pomieszczenia numery arabskie:	Szczególne kategorie danych (RODO) TAK/NIE	Dane z art. 10 RODO TAK/NIE
	1	2	3	4	5
1.					
2.					
3.					