DZIENNIK URZĘDOWY
MINISTRA ŚRODOWISKA
I GŁÓWNEGO INSPEKTORA OCHRONY ŚRODOWISKA

Załącznik do nru 4, poz. 79 z dnia 12 grudnia 2008 r.

TEKST ZAŁĄCZNIKA DO ZARZĄDZENIA MINISTRA ŚRODOWISKA

MINISTER ŚRODOWISKA

SPIS TREŚCI

Strona

Wydawca: Minister Środowiska i Główny Inspektor Ochrony Środowiska
Redakcja: Ministerstwo Środowiska, ul. Wawelska 52/54, 00-922 Warszawa
tel. 22 579-24-71, e-mail: Biuro.Edukacji.Ekologicznej.i.Komunikacji.Społecznej.@mos.gov.pl
Skład, druk i kolportaż: Centrum Obsługi Kancelarii Prezesa Rady Ministrów — Wydział Wydawnictw i Poligrafii,
ul. Powsińska 69/71, 02-903 Warszawa, tel. 22 694-67-52; faks 22 694-62-06
Bezpłatna infolinia: 0-800-287-581 (czynna w godz. 7^{30}–15^{30})
www.cokprm.gov.pl
e-mail: wydawnictwa@cokprm.gov.pl

Tłoczono z polecenia Ministra Środowiska i Głównego Inspektora Ochrony Środowiska w Centrum Obsługi Kancelarii Prezesa Rady Ministrów
Wydział Wydawnictw i Poligrafii, ul. Powsińska 69/71, 02-903 Warszawa

Zam. 806/W/C/2010

**Załącznik do zarządzenia Nr 56
Ministra Środowiska
z dnia 7 maja 2008 r.
(Dz. Urz. MŚiGIOŚ Nr 4, poz. 79)**

POLITYKA BEZPIECZEŃSTWA W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

w

Ministerstwie Środowiska

Warszawa 2008 r.

Spis treści

I. POSTANOWIENIA OGÓLNE

§ 1

Celem Polityki Bezpieczeństwa danych osobowych, zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania w Ministerstwie Środowiska informacji zawierających dane osobowe.

§ 2

Obszarem przetwarzania danych osobowych w Ministerstwie Środowiska są wydzielone pomieszczenia w budynku Ministerstwa, przy ul. Wawelskiej 52/54 w Warszawie.

§ 3

Określenia użyte w Polityce Bezpieczeństwa oznaczają:

1. Ministerstwo — Ministerstwo Środowiska.
2. Komórka organizacyjna — odpowiednio komórki organizacyjne, o których mowa w Statucie Ministerstwa Środowiska.
3. Dane osobowe — wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
4. Przetwarzanie danych osobowych — gromadzenie, utrwalanie przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych, zwłaszcza w systemach informatycznych.
5. Użytkownik — osoba upoważniona do przetwarzania danych osobowych.
6. Administrator systemu — osoba upoważniona do zarządzania systemem informatycznym.
7. System informatyczny — zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
8. Zabezpieczenie systemu informatycznego — wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych a także ich utratą.

II. DEFINICJA BEZPIECZEŃSTWA INFORMACJI

§ 4

1. Utrzymanie bezpieczeństwa przetwarzanych w Ministerstwie Środowiska informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.
2. Poniżej opisane jest rozumienie wyżej wymienionych pojęć w odniesieniu do informacji i aplikacji:
   1) poufność informacji — rozumiana jako zapewnienie, że tylko uprawnieni pracownicy mają dostęp do informacji;
   2) integralność informacji — rozumiana jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania;
   3) dostępność informacji — rozumiane jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
   4) zarządzanie ryzykiem — rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych.
3. Dodatkowo zarządzanie bezpieczeństwem informacji wiąże się z zapewnieniem:
   1) niezaprzeczalności odbioru — rozumianej jako zdolność systemu do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie;
   2) niezaprzeczalności nadania — rozumianej jako zdolność systemu do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym miejscu i czasie;
   3) rozliczalności działań — rozumianej, jako zapewnienie, że wszystkie działania istotne dla przetwarzania informacji zostały zarejestrowane w systemie i możliwym jest zidentyfikowanie użytkownika, który działania dokonał.

III. ZAKRES STOSOWANIA

§ 5

1. W Ministerstwie Środowiska przetwarzane są informacje służące do wykonywania zadań z zakresu administracji publicznej.

2. Informacje te są przetwarzane i składowane zarówno w postaci dokumentacji tradycyjnej jak i elektronicznej.

3. Polityka Bezpieczeństwa zawiera dokumenty dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

§ 6

Politykę Bezpieczeństwa stosuje się do:

1. Danych osobowych przetwarzanych w systemie: IRBIS, SPUWOJ, EXEL. Szczegółowe instrukcje dotyczące obsługi systemów baz danych znajdują się we właściwych komórkach organizacyjnych.

2. Danych osobowych gromadzonych w systemie zamówień publicznych.

3. Wszystkich informacji dotyczących danych pracowników Ministerstwo Środowiska, w tym danych osobowych personelu i treści zawieranych umów o pracę.

4. Wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji.

5. Informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych.

6. Rejestru osób dopuszczonych do przetwarzania danych osobowych.

7. Innych dokumentów zawierających dane osobowe.

§ 7

1. Zakresy ochrony danych osobowych określone przez dokumenty Polityki Bezpieczeństwa mają zastosowanie do systemów informatycznych Ministerstwa Środowiska, w których są przetwarzane dane osobowe, a w szczególności do:

   1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie;

   2) informacji będących własnością Ministerstwa Środowiska lub klientów Ministerstwa Środowiska, o ile zostały przekazane na podstawie umów;

   3) wszystkich lokalizacji — budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;

   4) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

2. Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy, konsultanci, stażyści oraz inne osoby mające dostęp do informacji podlegających ochronie.

§ 8

Informacje niejawne nie są objęte zakresem niniejszej Polityki Bezpieczeństwa.

IV. STRUKTURA DOKUMENTÓW POLITYKI BEZPIECZEŃSTWA

§ 9

1. Dokumenty Polityki Bezpieczeństwa ustanawiają metody zarządzania oraz wymagania niezbędne do zapewnienia skutecznej i spójnej ochrony przetwarzanych informacji.

2. Zestaw dokumentów Polityki Bezpieczeństwa składa się z:

   1) niniejszego dokumentu Polityki Bezpieczeństwa;

2) Instrukcji zarządzania systemami informatycznymi w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych, opisującej sposób zarządzania systemami przetwarzania danych osobowych w Ministerstwie Środowiska — załącznik nr 1;

3) Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych, opisującej tryb postępowania w sytuacjach naruszenia zabezpieczenia zasobów danych osobowych, zaobserwowanych prób naruszenia tego zabezpieczenia, a także uzasadnionego podejrzenia o przygotowywanej próbie naruszenia — załącznik nr 2;

4) Wykazu baz danych w systemach informatycznych, w których przetwarzane są dane osobowe w Ministerstwie Środowiska — załącznik nr 3 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, który powinien zawierać następujące pola:

a) liczba porządkowa,

b) nazwa bazy danych,

c) wersja bazy danych,

d) forma bazy danych/System operacyjny serwera,

e) sposób zabezpieczenia informatycznego,

f) czy zawiera także dane osób spoza MŚ,

g) czy baza danych jest chroniona przez UPS,

h) liczba miejsc przetwarzania i liczba porządkowa załączników;

5) Ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych i ich identyfikatorów — załącznik nr 2, do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ministerstwie Środowiska, która powinna zawierać następujące pola:

a) liczba porządkowa,

b) nazwa bazy danych,

c) nazwisko i imię użytkownika,

d) nazwa identyfikatora,

e) rodzaj uprawnień,

f) data zarejestrowania,

g) data wyrejestrowania,

h) lokalizacja,

i) uwagi;

6) Wykazu miejsc przetwarzania danych osobowych w systemach informatycznych — załącznik nr 3 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ministerstwie Środowiska, który powinien zawierać następujące pola:

a) liczba porządkowa,

b) nazwa bazy danych,

c) lokalizacja (piętro),

d) nr pokoju,

e) funkcja lokalizacji,

f) zabezpieczenie fizyczne;

7) Ponadto, w celu osiągnięcia jak najlepszej ochrony danych osobowych w Ministerstwie Środowiska, wprowadza się do stosowania następujące dokumenty dotyczące ich przetwarzania stanowiące załączniki do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ministerstwie Środowiska:

a) indywidualny zakres czynności osoby zatrudnionej przy przetwarzaniu danych osobowych — załącznik numer 4;

b) upoważnienie dotyczące obsługi systemu informatycznego w zakresie przetwarzania danych osobowych — załącznik numer 5;

c) protokół zniszczenia kopii bezpieczeństwa/innych nośników zawierających dane osobowe — załącznik numer 6;

d) dziennik ewidencji kopii bezpieczeństwa — załącznik numer 7;

e) dziennik pracy systemu serwera — załącznik numer 8;

f) oświadczenie (odpowiedzialność za sprzęt komputerowy oraz oprogramowanie) — załącznik numer 9;

g) wniosek o założenie profilu/nadanie uprawnień/modyfikację uprawnień — załącznik numer 10.

V. DOSTĘP DO INFORMACJI

§ 10

Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w Ministerstwie Środowiska zasad ochrony danych osobowych.

§ 11

Zakres czynności dla osoby dopuszczonej do przetwarzania danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę danych osobowych w stopniu odpowiednim do zadań tej osoby realizowanych przy przetwarzaniu tych danych.

§ 12

Udostępnianie danych osobowych podmiotom upoważnionym do ich otrzymania, na podstawie przepisów prawa, powinno odbywać się wg określonych odrębnymi przepisami procedur postępowania.

VI. BEZPIECZEŃSTWO INFORMACJI

§ 13

W Ministerstwie Środowiska należy stosować następujące kategorie środków zabezpieczeń danych osobowych:

a) zabezpieczenia fizyczne:
- — całodobowy monitoring budynku Ministerstwa Środowiska,
- — pomieszczenia zamykane na klucz,
- — szafy z zamkami,

b) zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej:
- — przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach,
- — przetwarzanie danych osobowych następuje przez wyznaczone do tego celu osoby,
- — dokumenty zawierające dane osobowe zbędne do prowadzenia dalszych działań i które nie podlegają archiwizacji są niezwłocznie niszczone w sposób uniemożliwiający ich odczytanie,

c) zabezpieczenia organizacyjne:
- — osobami bezpośrednio odpowiedzialnymi za bezpieczeństwo danych są: użytkownicy, lokalni administratorzy danych, Administrator sieci informatycznych, Administrator Bezpieczeństwa Informacji (ABI),
- — Administrator Bezpieczeństwa Informacji, Administrator sieci informatycznych, lokalni administratorzy danych osobowych na bieżąco kontrolują z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą i z obowiązującymi procedurami, pracę pracowników odpowiedzialnych za przetwarzanie danych osobowych oraz systemu informatycznego,

d) zabezpieczenia informatyczne.

Nie rzadziej, niż raz na miesiąc są prowadzone przez ABI kontrole stanu bezpieczeństwa systemów informatycznych i przestrzegania zasad ochrony informacji. W przypadkach wykrycia rażących zaniedbań ABI sporządza ich opis w formie protokołu i raportu i niezwłocznie przedkłada je Ministrowi Środowiska.

§ 14

Ochronę danych osobowych w Ministerstwie Środowiska należy realizować z wykorzystaniem następujących minimalnych zabezpieczeń:

a) przyznawania indywidualnych identyfikatorów,

b) zapewnienie stopniowania uprawnień,

c) zapewnienia wymuszania zmiany haseł,

d) odnotowania daty pierwszego wprowadzenia danych w systemie,

e) odnotowania identyfikatora użytkownika wprowadzającego dane,

f) odnotowania sprzeciwu określonego w art. 32 ust. 1 pkt 8 ustawy o ochronie danych osobowych,

g) odnotowania źródła danych, w przypadku zbierania danych nie od osoby, której dane dotyczą,

h) odnotowania informacji o odbiorcach, którym dane zostały udostępnione, dacie i zakresie tego udostępnienia,

i) zapewnienie możliwości sporządzenia i wydrukowania raportu zawierającego dane osobowe wraz z informacjami o historii przetwarzania danych.

§ 15

1. W ramach zabezpieczenia danych osobowych ochronie podlegają:
   a) sprzęt komputerowy — serwer, komputery osobiste, drukarki i inne urządzenia zewnętrzne,
   b) oprogramowanie — kody źródłowe, programy użytkowe, systemy operacyjne, narzędzia wspomagające i programy komunikacyjne,
   c) dane zapisane na dyskach oraz dane podlegające przetwarzaniu w systemie,
   d) hasła użytkowników,
   e) pliki dziennych operacji systemowych i baz danych, kopie zapasowe i archiwa,
   f) użytkownicy i administratorzy, którzy obsługują i używają system,
   g) dokumentacja — zawierająca dane systemu, opisująca jego zastosowanie, przetwarzane informacje itp.,
   h) wydruki,
   i) związana z przetwarzaniem danych osobowych dokumentacja papierowa, z której dane są wprowadzane do systemu informatycznego lub też funkcjonują niezależnie od niego.
2. W systemie informatycznym obowiązują zabezpieczenia na poziomie wysokim, określonym przez rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
3. Przyjmuje się, że podstawowymi i zarazem najważniejszymi zastosowanymi środkami zabezpieczenia danych osobowych w systemach informatycznych w Ministerstwie Środowiska będą:
   a) hasła dostępu do systemu,
   b) hasła dostępu do aplikacji,
   c) wygaszacze ekranu.

VII. ZARZĄDZANIE DANYMI OSOBOWYMI

§ 16

Administratorem danych osobowych w Ministerstwie Środowiska jest Minister Środowiska.

§ 17

1. Za bezpieczeństwo danych osobowych w Ministerstwie Środowiska, odpowiadają:
   1) Administrator Danych Osobowych — Minister Środowiska;
   2) Administrator Bezpieczeństwa Informacji Ministerstwa Środowiska;
   4) Lokalni administratorzy danych;
   5) Administrator sieci informatycznych.
2. Administrator Bezpieczeństwa Informacji Ministerstwa Środowiska realizując Politykę Bezpieczeństwa ma prawo wydawać zalecenia regulujące kwestie związane z ochroną danych osobowych w Ministerstwie Środowiska.
3. W umowach zawieranych przez Ministerstwo Środowiska winny znajdować się postanowienia zobowiązujące podmioty zewnętrzne do ochrony danych osobowych udostępnionych przez Ministerstwo Środowiska.

§ 18

1. Obowiązki wynikające z ustawy o ochronie danych osobowych Minister Środowiska powierza lokalnym administratorom danych — dyrektorom komórek organizacyjnych — w zakresie podległych im pracowników, systemów informatycznych i posiadanych baz danych.

2. Dyrektorzy komórek organizacyjnych Ministerstwo Środowiska odpowiadają za realizację wymagań obowiązujących przepisów prawa dotyczących ochrony danych osobowych i są zobowiązani do współdziałania z Administratorem Bezpieczeństwa Informacji w zakresie swoich właściwości.

3. Dyrektorzy komórek organizacyjnych Ministerstwa Środowiska zobowiązani są do zapoznania podległych pracowników z treścią ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.), Polityką Bezpieczeństwa w zakresie przetwarzania danych osobowych, Instrukcją zarządzania systemami informatycznymi w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych oraz Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych.

4. Zapoznanie się z dokumentami określonymi w ust. 3 pracownicy Ministerstwa Środowiska potwierdzają podpisem na „Indywidualnym zakresie czynności osoby zatrudnionej przy przetwarzaniu danych osobowych" (wzór w załączniku nr 4 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ministerstwie Środowiska). „Zakres czynności" przygotowywany jest w trzech egzemplarzach — jeden dla pracownika, jeden dla komórki właściwej w sprawach kadr, jeden dla Administratora Bezpieczeństwa Informacji.

5. Organizacja pracy przy przetwarzaniu danych osobowych i zasady przetwarzania:

   a) wykaz pracowników Ministerstwa Środowiska uprawnionych do przetwarzania danych osobowych, znajduje się u Administratora Bezpieczeństwa Informacji,

   b) przetwarzać dane osobowe mogą jedynie pracownicy, którzy zostali zapoznani z obowiązującymi zasadami dotyczącymi ochrony danych osobowych, potwierdzili fakt przeszkolenia przez lokalnego administratora danych lub ABI własnoręcznym podpisem i posiadają stosowne upoważnienie przyznane przez Administratora Danych Osobowych,

   c) w czasie przetwarzania danych osobowych, pracownik jest osobiście odpowiedzialny za bezpieczeństwo powierzonych mu danych,

   d) przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych, pracownik winien sprawdzić, czy posiadane przez niego dane były należycie zabezpieczone, oraz czy zabezpieczenia te nie były naruszone,

   e) w czasie przetwarzania danych osobowych, pracownik winien dbać o należyte ich zabezpieczenie przed możliwością wglądu, bądź zmiany przez osoby do tego celu nieupoważnione,

   f) po zakończeniu przetwarzania danych pracownik winien należycie zabezpieczyć dane osobowe przed możliwością dostępu do nich osób nieupoważnionych,

   g) pracownicy przetwarzający dane osobowe są bezpośrednio nadzorowani przez lokalnych administratorów danych osobowych,

   h) przetwarzanie danych osobowych w Ministerstwie Środowiska jest okresowo kontrolowane przez Administratora Bezpieczeństwa Informacji,

   i) zmiany oprogramowania, aktualizacji oprogramowania oraz jego zabezpieczenia antywirusowe i sieciowe dokonuje Administrator sieci informatycznych.

§ 19

Ochrona zasobów danych osobowych Ministerstwa Środowiska jako całości przed ich nieuprawnionym użyciem lub zniszczeniem jest jednym z podstawowych obowiązków pracowników Ministerstwa Środowiska.

VIII. ZAKRESY ODPOWIEDZIALNOŚCI

§ 20

Za bezpieczeństwo informacji odpowiedzialny jest każdy pracownik Ministerstwa Środowiska w zakresie zajmowanego stanowiska i posiadanych informacji.

§ 21

Administrator Bezpieczeństwa Informacji w Ministerstwie Środowiska:

1. Odpowiada za ochronę danych osobowych określonych w zakresie określonym w § 36 ust. 1 ustawy oraz Polityce Bezpieczeństwa Ministerstwa Środowiska.
2. Sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których dane są przetwarzane oraz kontrolą przebywających w nich osób.
3. Określa strategię zabezpieczania systemów informatycznych Ministerstwa Środowiska.
4. Identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych Ministerstwa Środowiska.
5. Określa potrzeby w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe.
6. Sprawuje nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe.
7. Monitoruje działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych.
8. Sprawuje nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane oraz kontrolą dostępu do danych.
9. Zatwierdza wniosek dyrektora komórki organizacyjnej o przyznaniu nowemu użytkownikowi identyfikatora oraz praw dostępu do informacji chronionych w danym systemie informatycznym.
10. Prowadzi ewidencję baz danych w systemach informatycznych, w których przetwarzane są dane osobowe.
11. Prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych.
12. Prowadzi ewidencję miejsc przetwarzania danych osobowych w systemach informatycznych.
13. Prowadzi rejestr zbiorów danych osobowych Ministerstwa Środowiska (przetwarzanych metodą tradycyjną lub w systemach informatycznych).

§ 22

Lokalni administratorzy danych osobowych zobowiązani są do przestrzegania wszystkich przepisów ustawy o ochronie danych, w szczególności poprzez:

1. Określanie indywidualnych obowiązków i odpowiedzialności osób zatrudnionych przy przetwarzaniu danych osobowych, wynikających z ustawy o ochronie danych osobowych.
2. Zapoznawanie osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami obowiązującymi w tym zakresie.
3. Wykonywanie zaleceń Administratora Bezpieczeństwa Informacji Ministerstwa Środowiska w zakresie organizacyjnej i technicznej ochrony danych osobowych.
4. Przekazywanie na bieżąco do Administratora Bezpieczeństwa Informacji zaktualizowanych załączników nr 1, 2, 3, do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
5. Wdrażanie i nadzorowanie przestrzegania Polityki Bezpieczeństwa.
6. Wdrażanie i nadzorowanie przestrzegania instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
7. Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe.
8. Sprawowanie nadzoru nad bezpieczeństwem danych zawartych w komputerach przenośnych, dyskach wymiennych, laptopach, w których przetwarzane są dane osobowe.
9. Podejmowanie działań określonych w instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych.

10. Tworzenie warunków organizacyjnych i technicznych umożliwiających spełnienie wymogów wynikających z obowiązywania ustawy o ochronie danych osobowych.

11. Nadzór nad poprawnością merytoryczną danych gromadzonych w systemach informacyjnych.

12. Określanie, które osoby i na jakich prawach mają dostęp do danych informacji.

13. Przygotowanie zgłoszeń rejestracji Zbiorów Danych do Generalnego Inspektoratu Danych Osobowych, jeżeli mają one charakter danych osobowych i przekazanie do Administratora Bezpieczeństwa Informacji.

Praca lokalnych administratorów danych osobowych jest nadzorowana pod względem stosowania zasad bezpieczeństwa przetwarzania danych osobowych przez Administratora Bezpieczeństwa Informacji.

§ 23

Administrator Systemu Informatycznego odpowiedzialny jest za:

1. Bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych.

2. Optymalizację wydajności systemu informatycznego, baz danych, instalacje i konfiguracje sprzętu sieciowego i serwerowego.

3. Instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego.

4. Konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem.

5. Nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych.

6. Współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych.

7. Zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego.

8. Zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie.

9. Przeciwdziałanie próbom naruszenia bezpieczeństwa informacji.

10. Przyznawanie na wniosek lokalnego administratora danych, za zgodą Administratora Bezpieczeństwa Informacji ściśle określonych praw dostępu do informacji w danym systemie.

11. Wnioskowanie do Administratora Bezpieczeństwa Informacji w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń.

12. Zarządzanie licencjami, procedurami ich dotyczącymi.

13. Prowadzenie profilaktyki antywirusowej.

Praca Administratora systemu informatycznego jest nadzorowana pod względem przestrzegania ustawy o ochronie danych osobowych, rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz Polityki Bezpieczeństwa przez Administratora Bezpieczeństwa Informacji.

IX. PRZETWARZANIE DANYCH OSOBOWYCH

§ 24

Systemy informatyczne, służące do przetwarzania danych osobowych, muszą spełniać wymogi obowiązujących aktów prawnych regulujących zasady gromadzenia i przetwarzania danych osobowych.

§ 25

Do tworzenia kopii bezpieczeństwa danych osobowych w postaci elektronicznej służą indywidualne systemy archiwizowania dla poszczególnych systemów informatycznych.

§ 26

Kopie bezpieczeństwa oraz dokumenty papierowe zawierające dane osobowe przechowuje się w warunkach uniemożliwiających dostęp do nich osobom nieuprawnionym.

§ 27

Dokumentami, które normują procedury zarządzania systemem informatycznym służącym do przetwarzania danych osobowych są instrukcje stanowiące załączniki do niniejszej Polityki Bezpieczeństwa określające m.in.:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;

2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;

3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;

4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;

5) zasady niszczenia nośników elektronicznych i dokumentów tradycyjnych zawierających dane osobowe;

6) sposób realizacji wymogów odnotowywania przez system informatyczny informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia;

7) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji (w tym tradycyjnych) — a także ich likwidacji — służących do przetwarzania danych osobowych;

8) sposób, miejsce i okres przechowywania:

   a) elektronicznych nośników informacji zawierających dane osobowe,

   b) kopii zapasowych;

9) sposoby zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

X. ARCHIWIZOWANIE INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE

§ 28

Archiwizację dokumentów zawierających dane osobowe prowadzi się w odpowiednio zabezpieczonych pomieszczeniach i na właściwie zabezpieczonych nośnikach informatycznych lub tradycyjnych. Dane zbędne dla prowadzonych spraw są natychmiast niszczone poprzez działania fizyczne i informatyczne uniemożliwiające ich odczytanie.

XI. POSTANOWIENIA KOŃCOWE

Administrator Bezpieczeństwa Informacji okresowo będzie analizował zagrożenia i ryzyko w celu weryfikacji środków zabezpieczających, a także dokonywał inwentaryzacji systemów informatycznych i zbiorów danych w celu zapewnienia aktualności opisowi zawartemu w punktach II—V Polityki Bezpieczeństwa.

Załączniki do Polityki Bezpieczeństwa w zakresie przetwarzania danych osobowych w Ministerstwie Środowiska

Załącznik nr 1

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

w

Ministerstwie Środowiska

Warszawa 2008 r.

Spis treści

I. POSTANOWIENIA OGÓLNE

§ 1

1. Instrukcja określa procedury zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, zwanych dalej danymi, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji w Ministerstwie Środowiska zwanym dalej Ministerstwem.
2. Instrukcja pozwala stosować ujednolicone zasady ochrony danych w systemach i sieciach informatycznych Ministerstwa.
3. Celem utworzenia instrukcji jest podniesienie poziomu bezpieczeństwa systemów informatycznych, w których są gromadzone i przetwarzane dane oraz określenie odpowiedzialności pracowników Ministerstwa za prawidłowe działanie tych systemów i bezpieczeństwo przetwarzanych w nim danych.

§ 2

Instrukcja w szczególności zawiera:

1. Określenie procedury przydziału haseł dla użytkowników i częstotliwość ich zmiany, ze wskazaniem osoby odpowiedzialnej za te czynności.
2. Określenie procedury rejestrowania i wyrejestrowywania użytkowników oraz wskazanie osoby odpowiedzialnej za te czynności.
3. Procedury rozpoczęcia i zakończenia pracy w systemach informatycznych.
4. Opis metod oraz procedurę i harmonogram tworzenia kopii bezpieczeństwa.
5. Opis metod i harmonogram sprawdzania obecności wirusów komputerowych oraz metody ich usuwania.
6. Procedurę i okres przechowywania elektronicznych nośników informacji i wydruków.
7. Procedurę i harmonogram dokonywania przeglądów i konserwacji systemów oraz zbiorów danych osobowych.
8. Zasady wyposażania i eksploatacji stacji roboczych.
9. Zasady wymiany informacji w sieciach komputerowych.

§ 3

Określenia użyte w instrukcji oznaczają:

1. Ustawa — Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.).
2. Rozporządzenie — Rozporządzenie 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 informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).
3. Ministerstwo — Ministerstwo Środowiska w Warszawie.
4. Komórka organizacyjna — odpowiednio komórki organizacyjne, o których mowa w § 2 „Statutu Ministerstwa Środowiska”.
5. Naruszenie bezpieczeństwa systemu informatycznego — jakiekolwiek naruszenie poufności, integralności, dostępności do systemu informatycznego spowodowane przez ludzi, jak też powstałe na skutek oddziaływania sił przyrody, katastrof itp.
6. Administrator Danych Osobowych — Minister Środowiska.
7. ABI — Administrator Bezpieczeństwa Informacji.
8. Administrator systemu informatycznego — osoba zarządzająca bieżącą pracą systemu informatycznego i zbiorami danych w Ministerstwie Środowiska.
9. Systemy informatyczne Ministerstwa Środowiska zwane dalej systemami — zespoły współpracujących ze sobą urządzeń, programów, procedur gromadzenia i przetwarzania informacji, narzędzi programowych zastosowanych do przetwarzania danych wraz ze zgromadzonymi danymi oraz osobami upoważnionymi do pracy na tych systemach (w tym obsługa techniczna urządzeń).

10. Przetwarzanie danych — jakiekolwiek operacje wykonywane na danych, takie jak utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, przekazywanie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

11. Obszar przetwarzania danych — obiekty, pomieszczenia komórek organizacyjnych Ministerstwa, w których odbywa się gromadzenie i przetwarzanie danych w układach elektronicznych na nośnikach magnetycznych, optycznych (również w postaci papierowej np. kartoteki czy inne zbiory informacji), urządzenia, elementy techniczne, z których charakteru pracy wynika wydawanie informacji na zewnątrz tzn. monitory, drukarki itp.

12. Zabezpieczenie danych w systemie Ministerstwa — wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym pozyskiwaniem, gromadzeniem i przetwarzaniem.

13. Użytkownik systemu zwany dalej użytkownikiem:

    1) osoba zatrudniona przy przetwarzaniu danych w Ministerstwie, która posiada upoważnienie do obsługi systemu oraz urządzeń wchodzących w jego skład, a także osoba przetwarzająca dane w toku wykonywania umowy cywilnoprawnej zawartej z Ministerstwem (np. umowy zlecenia, umowy o dzieło itp.);

    2) pracownik innego podmiotu, który świadczy usługi związane z pracą w systemie Ministerstwa, na podstawie odrębnych umów z tym podmiotem (np. serwis, zlecenie przetwarzania danych itp.).

14. Gromadzenie danych — zbieranie na nośnikach elektronicznych oraz wydrukach danych.

§ 4

1. Ochrona zasobów danych Ministerstwa jako całości, przed ich nieuprawnionym użyciem lub zniszczeniem, jest jednym z podstawowych obowiązków każdego pracownika Ministerstwa.

2. Obowiązkiem każdego pracownika Ministerstwa jest zachowanie tajemnicy służbowej, w tym ochrony danych osobowych gromadzonych i przetwarzanych przez Ministerstwo. Obowiązek ten istnieje również po ustaniu zatrudnienia.

3. Osoby zatrudnione przy przetwarzaniu danych osobowych (także poza systemami) są zobowiązane do szczególnej dbałości o zachowanie poufności, integralności i dostępności do danych gromadzonych w kartotekach, skorowidzach itp. oraz infrastruktury sprzętowo-programowej systemu.

§ 5

Za bezpieczeństwo danych osobowych Ministerstwa, odpowiadają:

1) Administrator danych osobowych — Minister Środowiska;

2) Administrator Bezpieczeństwa Informacji;

3) Administrator systemu informatycznego;

4) Lokalni administratorzy danych osobowych — dyrektorzy komórek organizacyjnych, oraz inne osoby zobowiązane do ochrony informacji na mocy innych przepisów.

§ 6

Obowiązki wynikające z ustawy o ochronie danych osobowych Minister Środowiska powierza lokalnym administratorom danych osobowych — dyrektorom komórek organizacyjnych — w zakresie podległych im pracowników.

§ 7

1. Obszary przetwarzania danych w obiektach i pomieszczeniach Ministerstwa nie mogą być dostępne dla osób nieuprawnionych.

2. Dopuszczalne odstępstwo stanowią pomieszczenia, w których przyjmowani są interesanci. Jeżeli pomieszczenia te wyposażone są jednocześnie w urządzenia z dostępem do systemów bazodanowych albo tradycyjne kartoteki, należy w nich stosować szczególne środki ostrożności, w tym:

    1) interesanci powinni wchodzić pojedynczo i pozostawać w pomieszczeniu tylko w obecności użytkownika systemu;

    2) kartoteki tradycyjne należy zabezpieczyć przed dostępem osób nieuprawnionych;

3) nie należy pozostawiać dokumentów papierowych i nośników elektronicznych w miejscach umożliwiających ich wykorzystanie, przez osoby nieuprawnione;

4) monitory powinny być usytuowane tak, aby ekrany były niewidoczne dla osób nieuprawnionych;

5) drukarki i urządzenia peryferyjne powinny być usytuowane tak, aby znajdowały się z dala od przestrzeni, po której poruszają się osoby nieuprawnione.

§ 8

Systemy informatyczne w Ministerstwie powinny być tak zaprojektowane, aby wymuszać autoryzację osoby przystępującej do pracy na zbiorach danych osobowych.

§ 9

Odpowiedzialność za ochronę danych zawartych na komputerach przenośnych i innych przenośnych urządzeniach umożliwiających gromadzenie danych, spoczywa wyłącznie na dysponentach tych urządzeń; minimalnym wymaganym zabezpieczeniem każdego komputera PC w Ministerstwie jak również komputera przenośnego jest ograniczenie dostępu do tego komputera hasłem (hasło na BIOS, Windows, wygaszasz ekranu).

§ 10

1. Dane wyeksportowane z systemu do komputera przenośnego mogą znajdować się na tym komputerze tylko przez niezbędny do ich wykorzystania czas.

2. Po wykorzystaniu danych określonych w ust. 1 należy je niezwłocznie usunąć.

3. Danych określonych w ust. 1 nie można udostępniać osobom nieuprawnionym.

§ 11

1. Wszelkie informacje zawierające dane, udostępniane podmiotom zewnętrznym Ministerstwa, mogą zostać przekazane tylko za pośrednictwem kancelarii ogólnej Ministerstwa.

2. W uzasadnionych przypadkach dane mogą być przesyłane drogą elektroniczną w formie zaszyfrowanej.

§ 12

1. Zabrania się:

1) zapisywania indywidualnych haseł dostępu;

2) dokonywania samowolnych napraw sprzętu informatycznego oraz modyfikowania oprogramowania;

3) samodzielnego zakupu sprzętu komputerowego lub oprogramowania;

4) autoryzacji w systemie jako inny użytkownik;

5) samodzielnego wgrywania oprogramowania;

6) w celach innych niż służbowe, wynoszenia dokumentacji, w tym na nośnikach elektronicznych zawierającej dane, poza obszar jednostki organizacyjnej;

7) instalowania na komputerach Ministerstwa prywatnych kont poczty elektronicznej;

8) wykorzystywania Internetu do celów innych niż służbowe oraz przeglądania nielegalnych stron z kodami aktywacyjnymi do programów lub programami łamiącymi zabezpieczenia programów przed nielegalnym kopiowaniem;

9) korzystania z czatów internetowych oraz ściągania innych plików.

2. Odwiedzanie stron internetowych jest monitorowane przez komórkę organizacyjną właściwą w sprawach informatyki Ministerstwa.

3. Identyfikator i hasło osoby, która utraciła uprawnienia do korzystania z systemu należy bezzwłocznie unieważnić.

4. Identyfikator osoby, która utraciła uprawnienia i została wyrejestrowana z systemu nie może być przydzielony innej osobie.

5. Dostęp do poszczególnych elementów systemów bazodanowych powinien być realizowany tylko w zakresie określonym nadanymi uprawnieniami, po wydaniu upoważnienia użytkownikowi.

§ 13

1. Osoby zatrudnione w Ministerstwie potwierdzają własnoręcznym podpisem zapoznanie się z indywidualnym zakresem czynności osoby zatrudnionej przy przetwarzaniu danych osobowych (wzór w załączniku nr 5 do niniejszej Instrukcji).

2. Osoby zatrudnione w Ministerstwie podlegają szkoleniu w zakresie ochrony danych osobowych, po którym otrzymują upoważnienie do obsługi systemów informatycznych w zakresie przetwarzania danych (wzór w załączniku nr 5 do niniejszej Instrukcji).

3. Upoważnienie do obsługi systemu w zakresie przetwarzania danych osobowych wydaje dyrektor komórki organizacyjnej właściwej w sprawach kadr, akceptuje Administrator Bezpieczeństwa Informacji oraz podpisuje Lokalny administrator danych.

4. Indywidualny zakres czynności (załącznik nr 4 — wzór) osoby zatrudnionej przy przetwarzaniu danych oraz Upoważnienie do obsługi systemów informatycznych w zakresie przetwarzania danych załącza się do akt personalnych pracownika.

§ 14

1. Administrator Bezpieczeństwa Informacji prowadzi następujące ewidencje:

   1) ewidencję baz danych w systemach informatycznych, w których przetwarzane są dane osobowe (wzór w załączniku nr 1 do niniejszej Instrukcji);

   2) ewidencję osób upoważnionych do przetwarzania danych osobowych w systemach informatycznych (wzór w załączniku nr 2 do niniejszej Instrukcji);

   3) ewidencję miejsc przetwarzania danych osobowych w systemach informatycznych i sposobu ich zabezpieczania (wzór w załączniku nr 3 do niniejszej Instrukcji).

2. Lokalni administratorzy danych zobowiązani są do przekazywania do Administratora Bezpieczeństwa Informacji zaktualizowanych załączników nr 1, 2, 3, do dnia 15 każdego miesiąca wg stanu na miesiąc poprzedni.

3. Dyrektor komórki właściwej w sprawach kadr powiadamia Administratora Bezpieczeństwa Informacji o zamiarze wypowiedzenia umowy o pracę, lub ustaniu stosunku pracy z osobą zatrudnioną w Ministerstwie przy przetwarzaniu danych osobowych.

4. Administrator Bezpieczeństwa Informacji niezwłocznie powiadamia o faktach wynikających z ust. 3, osobę odpowiedzialną za nadawanie haseł i kodów dostępu. Kody dostępu i hasła są likwidowane w ciągu 24 godzin od ustania uprawnień lub zatrudnienia.

II. PROCEDURY REJESTROWANIA I WYREJESTROWYWANIA UŻYTKOWNIKÓW

§ 15

1. Pracownika Ministerstwa korzystającego z systemu i jego oprogramowania rejestruje się jako użytkownika.

2. Niedopuszczalna jest praca w systemie na koncie innego użytkownika.

§ 16

1. W celu zarejestrowania osoby jako użytkownika systemu, dyrektor komórki organizacyjnej Ministerstwa, w której zatrudniona jest osoba, kieruje wniosek do Administratora sieci informatycznych, w którym określa:

   1) konieczne uprawnienia (bądź zmianę, wycofanie uprawnień) ze szczególnym uwzględnieniem uprawnień do przetwarzania danych osobowych;

   2) informację o przeszkoleniu użytkownika w zakresie ochrony danych osobowych, potwierdzoną przez Administratora Bezpieczeństwa Informacji.

2. Założenie profilu, nadanie uprawnień, modyfikacja uprawnień użytkownika do systemu informatycznego następuje po przedłożeniu do Administratora Bezpieczeństwa Informacji wniosku (wzór w załączniku nr 10 do Instrukcji).

§ 17

1. Nadawanie i rozszerzanie uprawnień użytkowników, w porozumieniu z lokalnym administratorem danych osobowych, koordynuje Administrator Bezpieczeństwa Informacji, który zleca wykonanie w tym zakresie administratorowi systemu informatycznego.

2. Administrator systemu informatycznego w porozumieniu z Administratorem Bezpieczeństwa Informacji nadaje, nadzoruje i wycofuje uprawnienia.

§ 18

Identyfikator użytkownika powinien spełniać następujące wymagania:

1) długość minimum trzy znaki;

2) musi być niepowtarzalny w skali systemu;

3) jednym identyfikatorem może posługiwać się tylko jeden użytkownik;

4) identyfikator jest natychmiast blokowany przez administratora systemu po rozwiązaniu z pracownikiem umowy o pracę, po uzyskaniu takiej informacji od Administratora Bezpieczeństwa Informacji;

5) identyfikator pracownika, który rozwiązał umowę o pracę nie może zostać przydzielony innemu pracownikowi.

III. BUDOWA I PROCEDURA PRZYDZIAŁU HASEŁ DLA ADMINISTRATORÓW SYSTEMÓW I UŻYTKOWNIKÓW ORAZ CZĘSTOTLIWOŚĆ ICH ZMIANY

§ 19

Określa się następujące zasady tworzenia haseł.

1. Hasło musi mieć nie mniej niż 8 znaków.

2. Hasło musi zawierać znaki z wszystkich trzech niżej wymienionych grup:

   1) małe i duże litery;

   2) cyfry;

   3) znaki specjalne.

3. W haśle nie wolno używać polskich znaków diakrytycznych lub innych znaków narodowych.

4. Hasło nie może mieć charakteru słownikowego.

5. Hasło jest obowiązkowe dla każdego użytkownika, posiadającego identyfikator w systemie.

6. Po założeniu hasła przez administratora użytkownik ma obowiązek zarejestrować się do systemu i zmienić hasło.

§ 20

Określa się następujące zasady korzystania z haseł:

1) nie wolno powtórnie używać hasła raz użytego;

2) hasło znane jest tylko użytkownikowi;

3) przy wpisywaniu hasła nie jest ono wyświetlane na ekranie;

4) użytkownik odpowiada za systematyczną zmianę haseł.

§ 21

Niedopuszczalne jest:

1) jakiekolwiek notowanie hasła;

2) podawanie swojego hasła innym użytkownikom systemu bądź osobom nie uprawnionym do pracy w systemie lub nie posiadającym uprawnień do przetwarzania danych.

§ 22

1. Hasła w systemach Ministerstwa zmienia się nie rzadziej niż raz na trzy miesiące.

2. Powyższe zalecenie jest obowiązujące w Ministerstwie niezależnie od tego czy użytkownik przetwarza dane.

§ 23

1. Administrator systemu informatycznego tworzy i zmienia hasła zgodnie z zasadami określonymi w niniejszej Instrukcji.

2. Hasła do serwerów, aktywnych urządzeń sieci i istotnych programów konfiguracyjnych, Administrator systemu informatycznego umieszcza w zapieczętowanych kopertach i składa w obecności Administratora Bezpieczeństwa Informacji w sejfie komórki organizacyjnej właściwej w sprawach informatyki Ministerstwa.

3. Otwarcie koperty określonej w ust. 2 może nastąpić w przypadku:

   1) kontroli prowadzonej przez Administratora Danych Osobowych;

   2) zamiaru zniszczenia nieaktualnych haseł przez Administratora systemów informatycznych;

   3) zaistnienia konieczności zapoznania się z jej zawartością spowodowanej rezygnacją z pracy, pozbawieniem uprawnień lub śmiercią Administratora systemu informatycznego; uprawnienie w tym zakresie posiada Administrator Bezpieczeństwa Informacji;

   4) innym określonym w „Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych w Ministerstwie Środowiska".

§ 24

1. Hasło lokalnego administratora stacji roboczych pozostaje w wyłącznej dyspozycji Administratora sieci informatycznych lub wytypowanych przez niego i przeszkolonych pracowników komórkę organizacyjną właściwą w sprawach informatyki Ministerstwa.

2. Zabrania się nadawania użytkownikom stacji roboczych uprawnień administratora stacji roboczej.

§ 25

Zobowiązuje się Administratora sieci informatycznych do uruchomienia na stacjach lokalnych (roboczych) procedury automatycznego wymuszania przez te systemy zmiany hasła.

IV. PROCEDURA ROZPOCZĘCIA I ZAKOŃCZENIA PRACY W SYSTEMIE INFORMATYCZNYM

§ 26

1. Użytkownik systemu informatycznego Ministerstwa musi być zarejestrowany przez Administratora systemu jako użytkownik odpowiedniej aplikacji.

2. Włączając komputer w celu podjęcia pracy użytkownik dokonuje autoryzacji zgodnie z poleceniami wydawanymi przez system komputerowy ukazującymi się na ekranie monitora.

3. W przypadku pojawienia się trudności w autoryzacji, pomimo prawidłowo wykonanych czynności, użytkownik zobowiązany jest skontaktować się z Administratorem systemu informatycznego.

4. Jeżeli autoryzacja przebiegła prawidłowo, użytkownik dokonuje wyboru aplikacji, w której zamierza pracować.

§ 27

Obowiązkiem każdego pracownika jest dbałość o niepozostawianie stanowiska informatycznego z dostępem do systemów bazodanowych, bez należytego zabezpieczenia, a w tym:

1) opuszczając stanowisko pracy należy wylogować się z systemu;

2) w przypadku krótkotrwałych przerw w pracy należy zablokować stację roboczą.

§ 28

Kończąc pracę w systemie użytkownik zamyka wszystkie otwarte aplikacje, a następnie zamyka system postępując zgodnie z ukazującymi się na ekranie monitora komunikatami.

V. OBSZARY PRZETWARZANIA DANYCH

§ 29

W celu zapewnienia bezpiecznych warunków przetwarzania danych w systemach Ministerstwa określa się obszary przetwarzania danych jako:

1) obiekty, wydzielone pomieszczenia lub części pomieszczeń, w których przetwarzane są dane (także w postaci tradycyjnej — papierowej);

2) części obiektów, w których znajdują się informatyczne urządzenia wyjścia (np. monitory, drukarki itp.).

§ 30

Pomieszczenie określone jako obszar przetwarzania danych powinno spełniać następujące warunki:

1) musi być wyposażone w zamek mechaniczny lub elektroniczny zamykany każdorazowo, gdy opuszczają je pracownicy zatrudnieni przy przetwarzaniu danych;

2) jeżeli pomieszczenie znajduje się na parterze, lub istnieje możliwość podglądu z zewnątrz, ekrany monitorów umieszcza się w sposób uniemożliwiający taki podgląd;

3) monitory komputerów, na których wykonuje się przetwarzanie danych powinny być ustawione w sposób uniemożliwiający ich podgląd osobom nieuprawnionym.

§ 31

Wydzielona część pomieszczenia określona jako obszar przetwarzania danych powinna spełniać następujące warunki:

1) wyposażenie (meble) w tej części pomieszczenia muszą być tak ustawione, aby uniemożliwić lub istotnie utrudnić dostęp do tego obszaru osobom nieuprawnionym;

2) monitory komputerów, na których dokonuje się przetwarzania danych powinny być ustawione w sposób uniemożliwiający ich podgląd osobom nieuprawnionym.

§ 32

1. Lokalni administratorzy danych (dyrektorzy komórek organizacyjnych Ministerstwa), sporządzają imienne wykazy pracowników komórki organizacyjnej aktualnie zatrudnionych przy przetwarzaniu danych (załącznik nr 2 do Instrukcji).

2. Lokalni administratorzy danych wykazy określone w ust. 1 przekazują do dnia 15 każdego miesiąca wg stanu na miesiąc poprzedni, Administratorowi Bezpieczeństwa Informacji.

§ 33

Nadzór nad przestrzeganiem zasad ochrony przetwarzanych danych sprawuje Administrator Bezpieczeństwa Informacji.

VI. OPIS METOD I HARMONOGRAM SPORZĄDZANIA KOPII BEZPIECZEŃSTWA

§ 34

1. Jedynie administrator systemów informatycznych jest upoważniony do sporządzania kopii zabezpieczających plików aplikacji i baz danych oraz systemów operacyjnych i ponosi pełną odpowiedzialność w tym zakresie.

2. Z kopii bezpieczeństwa mogą być odtwarzane zbiory danych, uprawnienia użytkowników i ustawienia związane ze specyfiką i uwarunkowaniami systemów Ministerstwa.

3. Odtwarzania dokonuje Administrator systemu informatycznego.

§ 35

1. Przyjmuje się zasadę, iż kopie bezpieczeństwa nie powinny być przechowywane w tym samym pomieszczeniu, w których przechowywane są zbiory danych eksploatowane na bieżąco.

2. Nośniki zawierające kopie bezpieczeństwa przechowywane są w sejfie ogniotrwałym.

3. Dostęp do kopii bezpieczeństwa może posiadać wyłącznie Administrator systemu informatycznego, a w razie jego nieobecności Administrator Danych Osobowych lub Administrator Bezpieczeństwa Informacji.

§ 36

1. Co najmniej raz na kwartał Administrator systemu informatycznego dokonuje sprawdzenia zasobów kopii bezpieczeństwa pod kątem ich przydatności do odtworzenia danych w przypadku awarii systemu.

2. Kopie bezpieczeństwa, które uległy uszkodzeniu, lub zdezaktualizowały się, podlegają bezzwłocznemu zniszczeniu.

3. Zniszczenia kopii bezpieczeństwa lub innego nośnika zawierającego dane, dokonuje się komisyjne na polecenie Administratora Bezpieczeństwa Informacji. Z wykonanych czynności sporządza się protokół zniszczenia (wzór protokołu w załączniku nr 6 do niniejszej Instrukcji).

§ 37

Opisu czynności sporządzania, okresowego sprawdzania, niszczenia kopii bezpieczeństwa, jak też odtwarzania danych z tych kopii, dokumentuje się w „Dzienniku ewidencji kopii bezpieczeństwa", który przechowywany jest przez Administratora systemu (wzór dziennika w załączniku nr 7 do niniejszej Instrukcji).

§ 38

Nadzór nad procesem sporządzania, przechowywania i niszczenia kopii bezpieczeństwa sprawuje Administrator Bezpieczeństwa Informacji.

§ 39

Sposób i częstotliwość tworzenia awaryjnych kopii systemu operacyjnego serwerów:

1. Kopia systemu operacyjnego powinna być wykonywana po każdej modyfikacji, zmianie, konfiguracji i instalacji nowej wersji oprogramowania.

2. Powinny istnieć przynajmniej dwa zestawy takiej kopii zapisywane naprzemiennie, kopie takie powinny być okresowo sprawdzane pod kątem ich przydatności — prawidłowości wykonania oraz możliwości odtwarzania.

§ 40

Metoda i częstotliwość tworzenia awaryjnych kopii danych:

1. Pełna kopia zabezpieczająca plików aplikacji i bazy danych systemów wykonywana jest raz w tygodniu.

2. Przyrostowa kopia zabezpieczająca wykonywana jest codziennie.

3. Każda kopia powinna zostać opisana w taki sposób, by zawierała następujące informacje:

   1) data wykonania;

   2) nazwa systemu informatycznego;

   3) nazwa zbioru danych.

VII. OPIS METOD ORAZ HARMONOGRAM SPRAWDZANIA OBECNOŚCI WIRUSÓW I ICH USUWANIE

§ 41

1. Bieżące sprawdzanie obecności wirusów komputerowych realizuje się przez stosowanie oprogramowania monitorującego występowanie wirusów.

2. Sprawdzaniu obecności wirusów podlegają wszystkie informatyczne nośniki danych.

3. Sprawdzanie obecności wirusów na dyskach serwerów przeprowadza Administrator systemów.

4. Administrator systemu informatycznego zobowiązany jest do zapewnienia systematycznej aktualizacji programu antywirusowego.

5. Sprawdzanie obecności wirusów na dyskach stacji roboczej odbywa się automatycznie po uruchomieniu komputera.

§ 42

1. O wykryciu wirusa na stacji roboczej użytkownik powiadamia Administratora systemu.

2. W przypadku problemów z usunięciem wirusa ze stacji roboczej użytkownik nie podejmuje dalszych działań do czasu przybycia Administratora systemu.

3. Administrator systemu informatycznego przypadku stwierdzenia szczególnie groźnych lub trudnych do usunięcia wirusów komputerowych powiadamia Administratora Bezpieczeństwa Informacji.

§ 43

Po dokonanej naprawie lub konserwacji należy przeprowadzić proces sprawdzenia pod kątem występowania wirusów.

§ 44

Informatyczne nośniki informacji pochodzenia zewnętrznego podlegają sprawdzeniu programem antywirusowym przed rozpoczęciem korzystania z nich.

§ 45

1. Nadzór nad prawidłowym funkcjonowaniem oprogramowania antywirusowego sprawuje Administrator systemu informatycznego.
2. Administrator systemu informatycznego zobowiązany jest do przeprowadzania systematycznej kontroli antywirusowej serwerów.

VIII. OGÓLNE ZASADY I ODPOWIEDZIALNOŚĆ PRZY INSTALACJI OPROGRAMOWANIA

§ 46

1. Administrator systemu informatycznego zobowiązany jest prowadzić dziennik czynności technologicznych serwera.
   W dzienniku tym opisuje się wszystkie czynności podejmowane w ramach jego administrowania, w szczególności związane z bezpieczeństwem danych osobowych (wzór dziennika w załączniku nr 8).
2. Do instalacji i modyfikacji oprogramowania na serwerach uprawniony jest wyłącznie Administrator systemu informatycznego.
3. O konieczności instalacji lub modyfikacji oprogramowania na serwerze decyduje Lokalny administrator danych osobowych.
4. Na serwerach może być instalowane tylko oprogramowanie, na które Ministerstwo posiada licencję.
5. Oprogramowanie testowe może być instalowane wyłącznie na wydzielonym serwerze lub systemie informatycznym.
6. Oprogramowanie testowe, odinstalowuje się bezzwłocznie po zakończeniu testowania.
7. Podczas prowadzenia testów oprogramowania, praca systemu jest na bieżąco monitorowana przez Administratora systemu.
8. Administrator systemu informatycznego prowadzący test oprogramowania niezwłocznie informuje o stwierdzonych nieprawidłowościach Lokalnego administratora danych osobowych i Administratora Bezpieczeństwa Informacji.

§ 47

1. Instalowanie oprogramowania testowego i bezpłatnego dopuszcza się pod warunkiem:
   1) otrzymania zgody na instalację od Lokalnego administratora danych osobowych;
   2) dokonania tego wyłącznie na stacjach roboczych będących w bezpośredniej dyspozycji komórki organizacyjnej właściwej w sprawach informatyki Ministerstwa.
2. O instalacji powiadamia się Administratora Bezpieczeństwa Informacji.

§ 48

Instalację lub modyfikację oprogramowania na serwerze lub stacji roboczej odnotowuje się na liście oprogramowania instalowanego.

§ 49

1. Administrator systemu informatycznego prowadzi wykaz oprogramowania dopuszczonego do używania w Ministerstwie.
2. Kontroli podlega rodzaj oprogramowania oraz ilość licencji zakupionych przez Ministerstwo.

§ 50

Zabrania się użytkownikom dokonywania samodzielnej instalacji jakiegokolwiek oprogramowania. Instalacji oprogramowania dokonują wyłącznie pracownicy komórki organizacyjnej właściwej w sprawach informatyki Ministerstwa.

§ 51

Na wszystkich komputerach w Ministerstwie dopuszcza się instalację tylko legalnego, licencjonowanego oprogramowania.

§ 52

Wprowadza się następujące zasady korzystania z oprogramowania:

1. Oryginalne dokumenty licencyjne oraz nośniki każdego oprogramowania przechowywane są w komórce Informatyki w zamkniętej szafie. Nośniki oprogramowania nie mogą znajdować się w żadnym innym miejscu, a szczególnie nie mogą być kopiowane, wypożyczane lub w żaden sposób przekazywane osobom trzecim. Dotyczy to również kodów aktywacyjnych produktów.

2. Każdy z pracowników zobowiązany jest do podpisania karty użytkownika (wzór w załączniku nr 9).

3. Zabrania się użytkownikom wykonywania kopii oprogramowania.

4. Wszyscy pracownicy zobowiązani są do pracy na legalnym oprogramowaniu oraz otrzymują wyraźny zakaz instalacji i użytkowania oprogramowania pochodzącego ze źródeł innych niż komórka organizacyjna właściwa w sprawach informatyki Ministerstwa.

5. Zakupy oprogramowania muszą być konsultowane z Lokalnym administratorem danych osobowych.

6. Do podstawowych obowiązków pracownika należy korzystanie z oprogramowania w związku z wykonywaniem obowiązków pracowniczych, zgodnie z obowiązującymi przepisami prawa oraz wyłącznie w celach wykonywania obowiązków pracowniczych. Zabrania się korzystania z jakiegokolwiek oprogramowania, do którego Ministerstwo nie jest uprawnione, w czasie pracy, w miejscu pracy i przy użyciu sprzętu Ministerstwa.

IX. PROCEDURA I OKRES PRZECHOWYWANIA NOŚNIKÓW INFORMACJI, W TYM KOPII ELEKTRONICZNYCH I WYDRUKÓW

§ 53

1. Nośniki informacji, w tym kopie elektroniczne i wydruki zawierające dane nie mogą być dostępne dla osób nieuprawnionych.

2. Dane z magnetycznych nośników informacji usuwa się bezzwłocznie po ich wykorzystaniu służbowym, w sposób trwały.

3. Zabrania się sporządzania kopii baz danych na dyskach twardych stacji roboczych lub w folderach ogólnodostępnych w systemach Ministerstwa.

§ 54

1. Użytkownik dokonujący wydruku jest właścicielem wytworzonego dokumentu.

2. Użytkownik dokonujący wydruku na drukarce sieciowej, zobowiązany jest udać się niezwłocznie do pomieszczenia usytuowania drukarki i przejąć drukowany dokument.

3. Kopie błędne, nadmiarowe czy z innych powodów niepotrzebne należy niezwłocznie zniszczyć.

4. Wydruki, które nie podlegają archiwizacji należy niezwłocznie zniszczyć.

5. Każdy pracownik, który napotka wydruk, nośnik elektroniczny, czy inny dokument pozostawiony bez dozoru jest zobowiązany zabezpieczyć go i przekazać Administratorowi Bezpieczeństwa Informacji.

§ 55

Wydruki zawierające dane sporządzane w oparciu o systemy Ministerstwa podlegają szczególnej ochronie, a w szczególności niedopuszczalne jest:

1) pozostawianie wydruków zawierających dane, z możliwością dostępu do nich osób nieuprawnionych;

2) wyrzucania nieudanych lub próbnych wydruków do kosza.

X. PROCEDURA I HARMONOGRAM DOKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ ZBIORÓW DANYCH

§ 56

Przeglądu i konserwacji systemu i zbioru danych dokonuje Administrator systemu informatycznego.

§ 57

1. Przegląd systemu polega na sprawdzeniu jego konfiguracji oraz sprawdzeniu logów systemowych, ze szczególnym uwzględnieniem logów bezpieczeństwa.
2. Przeglądu systemu dokonuje się codziennie.
3. W przypadku stwierdzenia nieprawidłowości w systemie, Administrator systemu informatycznego usuwa je, wykorzystując dostępne narzędzia i odnotowuje ten fakt w dzienniku pracy serwera (wzór w załączniku nr 8 do niniejszej Instrukcji).
4. Jeżeli stwierdzone nieprawidłowości wskazują na działanie osób nieuprawnionych w systemie, Administrator systemu informatycznego podejmuje czynności zgodnie z zapisami „Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych w Ministerstwie".

§ 58

1. Przegląd zbiorów danych polega na:
   1) sprawdzeniu dostępu do zbiorów danych na poziomie użytkowników o różnych prawach dostępu;
   2) ocenie stanu zbiorów danych;
   3) sprawdzeniu ustawień dostępu dla poszczególnych użytkowników.
2. Przeglądu zbiorów danych dokonuje się codziennie.
3. W przypadku stwierdzenia nieprawidłowości w stanie zbiorów danych lub naruszenia praw dostępu, Administrator systemu informatycznego powiadamia o zaistniałym fakcie Administratora Bezpieczeństwa Informacji, a następnie podejmuje działania zmierzające do usunięcia nieprawidłowości i zidentyfikowania osoby, która doprowadziła do ich powstania.
4. W przypadku wykrycia użytkowników nieuprawnionych, których działania mogły doprowadzić do: przeglądania, przenikania, wnioskowania, zniekształcania, powtarzania, wstawiania, niszczenia, kradzieży, modyfikacji, szpiegostwa, blokowania usług systemu itp., Administrator systemu informatycznego podejmuje czynności zgodnie z zapisami „Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych w Ministerstwie".

XI. ZASADY WYPOSAŻANIA I EKSPLOATACJI STACJI ROBOCZYCH

§ 59

1. Zasadność zakupu sprzętu komputerowego oraz oprogramowania podlega ocenie i akceptacji przez Lokalnego administratora danych osobowych.
2. Lokalny administrator danych osobowych nadzoruje proces zakupu sprzętu komputerowego oraz oprogramowania.
3. Instalacja sprzętu komputerowego na stanowiskach pracy wykonywana jest przez pracowników komórki organizacyjnej właściwej w sprawach informatyki Ministerstwa.
4. Każdy z pracowników pracujący przy przetwarzaniu danych osobowych, którego stanowisko pracy zostało wyposażone w sprzęt komputerowy zobowiązany jest podpisać oświadczenie o zapoznaniu się ze specyfikacją powierzonego sprzętu komputerowego oraz oprogramowania (wzór w załączniku nr 9).
5. Przeniesienia sprzętu do innych pomieszczeń wykonywane będą przez pracowników komórki organizacyjnej właściwej w sprawach informatyki Ministerstwa na wniosek Dyrektora komórki organizacyjnej. Zabrania się samodzielnego przenoszenia sprzętu przez innych pracowników.
6. Zmiana osoby odpowiedzialnej za powierzony sprzęt musi być zgłoszona przez Dyrektora komórki organizacyjnej do pracowników komórki organizacyjnej właściwej w sprawach informatyki Ministerstwa.
7. Zasady korzystania przez pracowników z oprogramowania Ministerstwa zostały opisane w § 52.

XII. ZASADY WYMIANY INFORMACJI W SIECI KOMPUTEROWEJ

§ 60

1. Użytkownik systemu Ministerstwa zobowiązany jest do prawidłowego rozpoczęcia i zakończenia pracy w systemie.

2. System Ministerstwa powinien być przygotowany do przekazywania informacji zawierających dane osobowe pomiędzy poszczególnymi komórkami organizacyjnymi i uprawnionymi podmiotami zewnętrznymi za pośrednictwem poczty elektronicznej z obowiązkiem szyfrowania.

3. Zabrania się wykorzystywania poczty elektronicznej do przekazywania dokumentów zawierających dane, bez odpowiedniego sposobu zaszyfrowania.

XIII. POSTANOWIENIA KOŃCOWE

§ 61

Przestrzeganie postanowień niniejszej Instrukcji przez użytkowników systemów stanowi podstawę bezpiecznego posługiwania się systemami Ministerstwa.

§ 62

Instrukcja nie może być wynoszona z obiektów Ministerstwa, powielana w części lub całości bez zgody Administratora Bezpieczeństwa Informacji.

§ 63

1. Postanowienia niniejszej Instrukcji mogą być modyfikowane zarządzeniem Ministra.

2. Propozycje zmian może składać pisemnie każdy pracownik Ministerstwa korzystając z drogi służbowej lub bezpośrednio do Administratora Bezpieczeństwa Informacji.

§ 64

Administrator Bezpieczeństwa Informacji okresowo monitoruje przestrzeganie przez pracowników Ministerstwa zasad i przepisów ochrony danych osobowych.

§ 65

W kwestiach nie uregulowanych niniejszą Instrukcją mają zastosowanie unormowania Regulaminu Pracy Ministerstwa, przepisy Kodeksu Pracy i Ustawy o ochronie danych osobowych wraz z aktami wykonawczymi.

XIV. SPIS ZAŁĄCZNIKÓW

Załącznik nr 1 — Wykaz baz danych w systemach informatycznych, w których przetwarzane są dane osobowe w Ministerstwie Środowiska

Załącznik nr 2 — Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych i ich identyfikatorów

Załącznik nr 3 — Wykaz miejsc przetwarzania danych osobowych w systemach informatycznych w Ministerstwie Środowiska

Załącznik nr 4 — Indywidualny zakres czynności osoby zatrudnionej przy przetwarzaniu danych osobowych

Załącznik nr 5 — Upoważnienie do obsługi systemu informatycznego w zakresie przetwarzania danych osobowych

Załącznik nr 6 — Protokół zniszczenia kopii bezpieczeństwa/innych nośników zawierających dane osobowe

Załącznik nr 7 — Dziennik ewidencji kopii bezpieczeństwa

Załącznik nr 8 — Dziennik pracy systemu serwera

Załącznik nr 9 — Oświadczenie (odpowiedzialność za sprzęt komputerowy oraz oprogramowanie)

Załącznik nr 10 — Wniosek o założenie profilu/nadanie uprawnień/modyfikację uprawnień

Załącznik nr 2

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Za naruszenie ochrony danych osobowych uznaje się przypadki, gdy:

stwierdzono naruszenie zabezpieczenia systemu informatycznego, lub:

stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.

Każdy pracownik Ministerstwa Środowiska, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie informatycznym ministerstwa zobowiązany jest do niezwłocznego poinformowania o tym administratora systemu informatycznego, lokalnego administratora danych osobowych lub w przypadku ich nieobecności Administratora Bezpieczeństwa Informacji Ministerstwa Środowiska.

Lokalny administrator danych osobowych, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony bazy danych zobowiązany jest do niezwłocznego:

1) zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnym wykryciu tego faktu;

2) jeżeli zasoby systemu na to pozwalają, wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania;

3) przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych itp.;

4) podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych, w tym m.in.:

   a) fizycznego odłączenia urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie niepowołanej,

   b) wylogowania użytkownika podejrzanego o naruszenie ochrony danych,

   c) zmianę hasła na konto administratora, użytkownika poprzez którego uzyskano nielegalny dostęp w celu uniknięcia ponownej próby uzyskania takiego dostępu;

5) szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych;

6) przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, odtworzenia jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną, tą samą drogą.

Po przywróceniu normalnego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

Jeżeli przyczyną zdarzenia był błąd użytkownika systemu informatycznego, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych.

Jeżeli przyczyną zdarzenia była infekcja wirusem należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne wykluczające powtórzenie się podobnego zdarzenia w przyszłości.

Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika systemu należy wyciągnąć konsekwencje dyscyplinarne wynikające z kodeksu pracy oraz ustawy o ochronie danych osobowych.

Lokalny administrator danych osobowych, w której nastąpiło naruszenie ochrony danych osobowych, przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia i w terminie 14 dni od daty jego zaistnienia przekazuje Administratorowi Bezpieczeństwa Informacji Ministerstwa Środowiska.

Administrator Bezpieczeństwa Informacji w Ministerstwie Środowiska przeprowadza analizę raportów pochodzących od lokalnych administratorów danych osobowych i uwzględnia je w opracowywanym corocznie raporcie dla Administratora Danych Osobowych w Ministerstwie Środowiska.

Załączniki do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ministerstwie Środowiska

Załącznik nr 1

.....
Nazwa komórki organizacyjnej

Wykaz baz danych w systemach informatycznych, w których przetwarzane są dane osobowe w Ministerstwie Środowiska

Lp.	Nazwa bazy danych(1)	Wersja bazy danych	Forma bazy danych/System operacyjny serwera(2)	Sposób zabezpieczenia informatycznego(3)	Zawiera także dane osób spoza MŚ (T/N)	Baza danych chroniona przez UPS (T/N)	Liczba miejsc przetwarzania i liczba porządkowa załączników

(1) nazwa zwyczajowa lub własna
(2) np. plik Excela/Windows 2000, lub baza MySQL/Mandrake 9.0, baza prowadzona w formie papierowej
(3) np. (I) indywidualne hasło dostępu do bazy danych, (S) szyfrowanie bazy danych, (F) wydzielona fizycznie sieć
(4) np. kontrola dostępu

Załącznik nr 2

.....
Nazwa komórki organizacyjnej

Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych i ich identyfikatorów

Lp.	Nazwa bazy danych(1)	Nazwisko i imię użytkownika	Nazwa identyfikatora	Rodzaj uprawnień(2)	Data zarejest.	Data wyrejest.	Lokalizacja(3)	Uwagi

(1) Nazwa bazy danych z załącznika nr 1
(2) Skróty stosowane do określenia uprawnień
Z — pełne prawa do zarządzania bazą danych
W — pełne prawa do edycji danych (w tym drukowania, archiwizowania, usuwania)
N — prawo do zakładania nowych kont
M — prawo do dodawania i modyfikacji danych
P — prawo do przeglądania danych na ekranie
D — prawo do drukowania danych
A — prawo do wykonywania kopii archiwalnych
Uwaga: w przypadku praw ograniczonych do określonej części bazy danych (np. studentów określonego kierunku studiów) należy ograniczenie to podać w polu Uwagi
(3) należy podać liczbę porządkową zgodnie z załącznikiem nr 3

Dane aktualne na dzień: ...../...../.....

Sporządził: .....

Załącznik nr 3

.....
Nazwa komórki organizacyjnej

Wykaz miejsc przetwarzania danych osobowych w systemach informatycznych w Ministerstwie Środowiska

UWAGA: do każdej lokalizacji należy dołączyć szkic sytuacyjny określający położenie stanowisk komputerowych w pomieszczeniu, z zaznaczeniem strefy ochronnej, do której nie mają dostępu osoby nieupoważnione, drzwi wejściowe, okna oraz zabezpieczenia fizyczne.

Lp.	Nazwa bazy danych(1)	Lokalizacja (piętro)	Nr pokoju	Funkcja lokalizacji(2)	Zabezpieczenie fizyczne(3)

(1) nazwa bazy danych z załącznika nr 5
(2) (S) — serwer, (K) — miejsce przechowywania kopii bezpieczeństwa, Z — pomieszczenie w którym wykonywane są kopie bezpieczeństwa, U — pomieszczenie osób wprowadzających dane, A — pomieszczenie administratora bazy danych
(3) (K) — kraty w oknach, (A) — alarm, (W) — wzmocnione drzwi

Załącznik nr 4

<table>
<tr><td>Nazwa i adres pracodawcy:

Ministerstwo Środowiska
w Warszawie
ul. Wawelska 52/54
00-911 Warszawa</td><td colspan="2">INDYWIDUALNY ZAKRES CZYNNOŚCI
NR ____/_____ OSOBY ZATRUDNIONEJ
PRZY PRZETWARZANIU
DANYCH OSOBOWYCH</td></tr>
<tr><td colspan="3">Imię i nazwisko pracownika:</td></tr>
<tr><td colspan="2">Stanowisko:</td><td>Pracuje na stanowisku od dnia:</td></tr>
<tr><td colspan="2">Nazwa komórki organizacyjnej:</td><td>Bezpośredni przełożony:</td></tr>
</table>

<u>Przetwarzanie danych</u> — rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych *(art. 7 pkt 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.)*.

<u>Dane osobowe</u> — wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej *(art. 6 ust.1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.)*.

- Obowiązkiem każdego pracownika Ministerstwa Środowiska jest zachowanie tajemnicy państwowej i służbowej, również w zakresie ochrony danych osobowych gromadzonych i przetwarzanych w Ministerstwie Środowiska. Obowiązek ten istnieje również po ustaniu zatrudnienia.
- Dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
- Dokumentów materialnych (w formie elektronicznej, papierowej itp.) z danymi osobowymi nie można pozostawiać bez dozoru, ani udostępniać osobom nieupoważnionym.
- Dokumentacji z danymi nie wolno wykorzystywać do innych celów niż służbowe.
- Dokumentacji z danymi nie wolno udostępniać osobom nieuprawnionym.
- Pracownik musi dopilnować, aby monitor usytuowany był tak, by ekran był niewidoczny dla osób wchodzących do pomieszczenia.
- Przy krótkotrwałych przerwach w pracy należy stosować blokady stacji roboczych.
- Pracownik może uzyskać dostęp do systemu tylko i wyłącznie jako użytkownik na swoje hasło. Ustala się czas, po którym system wymusza zmianę hasła na 30 dni.
- Oprogramowanie wgrywa tylko i wyłącznie administrator systemu informatycznego, nie wolno tego robić samodzielnie.
- Pracownik odpowiada za wykonany wydruk, ponieważ jest jego właścicielem. W przypadku wykonania wydruku z użyciem drukarki sieciowej osoba po wydaniu po jest obowiązana udać się niezwłocznie do pomieszczenia drukarki i przejąć drukowany dokument.
- Wydrukowane nadmiarowe, niepotrzebne lub błędne dokumenty należy niezwłocznie, trwale zniszczyć.
- Wszelkie informacje, w tym w formie tradycyjnej lub na nośnikach przesyłanych pocztą, zawierające dane osobowe wysyłane poza Ministerstwo Środowiska przekazane mogą zostać tylko po zarejestrowaniu przez kancelarię.

1. Oświadczam, że znana jest mi definicja danych osobowych w rozumieniu art. 6 Ustawy o ochronie danych osobowych z dnia 29.08.1997 r. (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.), w myśl której za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

2. Zostałam/em zaznajomiona/y z przepisami dotyczącymi ochrony danych osobowych, z „Polityką bezpieczeństwa informacji w zakresie przetwarzania danych osobowych w Ministerstwie Środowiska", „Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ministerstwie Środowiska" oraz „Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych", „Instrukcją określającą sposób rejestrowania i wyrejestrowania użytkownika, sposób przydziału haseł, komunikacji w sieci komputerowej osób pracujących przy przetwarzaniu danych osobowych w Ministerstwie Środowiska".

3. Zobowiązuję się, w przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie ochrony danych osobowych, bezzwłocznie powiadomić Administratora Bezpieczeństwa Informacji, lokalnego administratora danych, Administratora systemu informatycznego, a po godzinach urzędowania również ochronę obiektu.

4. Zobowiązuję, się przy przetwarzaniu danych osobowych, do szczególnej dbałości o zachowanie poufności, integralności i dostępności danych związanych z dokumentami znajdującymi się w obrocie w Ministerstwie Środowiska, także dotyczących danych osobowych pracowników, dokumentacji systemu przetwarzania danych oraz infrastruktury sprzętowo-programowej systemów informatycznych.

5. Zobowiązuję się przy przetwarzaniu danych, poza systemem informatycznym, do szczególnej dbałości o zachowanie poufności treści dokumentów, oraz przestrzegania zasad dostępu do danych osobowych.

Oświadczam, że treść niniejszego zakresu jest mi znana i zobowiązuję się do jego przestrzegania.

Wykonano w 3 egzemplarzach
Potwierdzam odbiór 1 egzemplarza

Warszawa, dnia .....

.....
(czytelny podpis pracownika)

Załącznik nr 5

Ministerstwo Środowiska

Warszawa, dnia .....

U P O W A Ż N I E N I E

dotyczące: obsługi systemu informatycznego w zakresie przetwarzania danych osobowych

Upoważniam Panią/na ..... zatrudnioną/ym

w Ministerstwie Środowiska na stanowisku: .....

od dnia ..... zgodnie z Art. 37 Ustawy o ochronie danych osobowych z dnia 29.08.1997 r. (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.) — do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych.

Administrator Danych Osobowych

.....
(data i podpis osoby upoważnionej)

Załącznik nr 6

WZÓR

.....
pieczęć nagłówkowa

.....
miejscowość, data

PROTOKÓŁ ZNISZCZENIA

kopii bezpieczeństwa*/innych nośników zawierających dane osobowe*

Nr: .....

Komisja w składzie:

1. .....

2. .....

3. .....
(imię, nazwisko, stanowisko)

Oświadcza, iż kopie bezpieczeństwa*/inne nośniki* otrzymane z .....
(nazwa komórki organizacyjnej)

zostały w dniu ..... komisyjnie zniszczone .....

.....
(opis procesu zniszczenia)

Rodzaj i oznaczenie nośników: .....

Ilość (szt.): .....

Uwagi: .....

.....

Podpisy komisji:

1. .....

2. .....

3. .....

* niepotrzebne skreślić

Załącznik nr 7

WZÓR

DZIENNIK EWIDENCJI KOPII BEZPIECZEŃSTWA

Lp.	Oznaczenie systemu/ zbioru danych	Określenie metody (całościowa, przyrostowa)	Oznaczenie nośnika, na którym utworzono kopię awaryjną	Kopię bezpieczeństwa utworzył:			Kopię bezpieczeństwa zniszczył:			Uwagi np. dot. odtwarzania
				Nazwisko i imię administratora systemu	Data	Podpis	Nazwisko i imię przewodniczącego komisji	Data	Podpis	
1	2	3	4	5	6	7	8	9	10	11

Załącznik nr 8

WZÓR

DZIENNIK PRACY SYSTEMU SERWERA .....

Lp.	Data	Godzina	Opis wykonywanych czynności	Podpis
1	2	3	4	5

Załącznik nr 9

Warszawa, dnia .....

.....
Imię i Nazwisko

.....
komórka organizacyjna

OŚWIADCZENIE

Oświadczam, że ponoszę pełną odpowiedzialność materialną za otrzymany sprzęt komputerowy oraz oprogramowanie, wg niniejszej specyfikacji:

Nazwa	Ilość	Oznaczenie w kartotece sprzętu komputerowego oraz oprogramowania
Jednostka centralna PC		
Monitor		
Klawiatura		
Mysz		
Drukarka		
UPS		
MS Windows		
MS Office		
Inne		

.....
podpis

Załącznik nr 10

Wniosek
o założenie profilu/nadanie uprawnień/modyfikację uprawnień*

Dane użytkownika

Nazwisko	
Imię	
Stanowisko służbowe	
Wydział	
Telefon stacjonarny	
e-mail	
Nr upoważnienia dot. obsługi systemu informatycznego w zakresie przetwarzania danych osobowych	

Wnioskuję o:

założenie profilu i nadanie uprawnień*)

modyfikację uprawnień na wymienione poniżej*)

zablokowanie profilu*)

Wnioskowane uprawnienia do systemu .....
(nazwa bazy danych)[1]

Uprawnienie, które ma być przyznane pracownikowi, należy zaznaczyć w pierwszej kolumnie znakiem „x".

TAK	Nazwa	Opis uprawnienia	Uwagi
	Z	Pełne prawa do zarządzania bazą	
	W	Pełne prawa do edycji danych (w tym drukowania, usuwania)	
	N	Prawo do zakładania nowych kont	
	M	Prawo do dodawania i modyfikacji danych	
	P	Prawo do przeglądania danych na ekranie	
	D	Prawo do drukowania danych	
	A	Prawo do wykonywania kopii archiwalnych	
	INNE		

Wniosek o nadanie/modyfikację uprawnień złożył:

Nazwisko i imię: _____ Dnia: / /

Podpis: _____

Oświadczam, że zostałem przeszkolony z zasad bezpieczeństwa przetwarzania danych osobowych i zobowiązuję się do ich przestrzegania.	Data, podpis użytkownika profilu
Upoważniam ww. pracownika do obsługi systemu informatycznego w zakresie przetwarzania danych osobowych zgodnie z Ustawą o ochronie danych osobowych z dnia 29.08.1997 r. (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.)	Data, podpis Administratora Bezpieczeństwa Informacji

Nadanie/modyfikację uprawnień wykonał:

Nazwisko i imię: _____ Dnia: / /

Podpis : _____

NADANO IDENTYFIKATOR: | | | | | | | | | |

---

* — niepotrzebne skreślić
1 — nazwa bazy danych z załącznika nr 1 do Instrukcji zarządzania systemami informatycznymi w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych w Ministerstwie Środowiska