Załącznik nr 6 do polityki ochrony danych osobowych

INSTRUKCJA
ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH
URZĄD GMINY I MIASTA GRYFÓW ŚLĄSKI

ROZDZIAŁ I
Postanowienia ogólne

§ 1

1. Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych, zwana dalej „Instrukcją", określa sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji, a także zasady i tryb postępowania Administratora Danych oraz osób przez niego upoważnionych związanego z przetwarzaniem danych osobowych.
2. Instrukcja została opracowana zgodnie z wymogami określonymi w Rozporządzeniu 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).

§ 2

Instrukcja określa stosowne procedury i warunki zarządzania systemem informatycznym oraz kartotekami, zapewniające ochronę przetwarzania danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

§ 3

Ilekroć w instrukcji jest mowa o:

1. Zbiorze danych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalne;
2. Przetwarzaniu danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, taki jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemie informatycznym;
3. Systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
4. Kartotece – rozumie się przez to zewidencjonowany, usystematyzowany zbiór wykazów, skoroszytów, wydruków komputerowych i innej dokumentacji gromadzonej w formie papierowej, zawierający dane osobowe;
5. Administratorze Danych – rozumie się przez to Urząd Gminy i Miasta Gryfów Śląski jako administratora danych przetwarzanych w Urzędzie Gminy i Miasta Gryfów Śląski;
6. Inspektora Ochrony Danych Osobowych – rozumie się przez to osobę wyznaczoną przez Administratora Danych nadzorującą przestrzegania zasad ochrony przetwarzania danych osobowych. Nadzór dotyczy przede wszystkim stosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenia danych przez ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem obowiązujących przepisów, oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Przeprowadza on również kontrole w zakresie określonym regulacjami wewnętrznymi obowiązującymi u Administratora Danych;

7. Administratorze Systemów Informatycznych (ASI) – rozumie się przez to osobę odpowiedzialną za prawidłowe funkcjonowanie sprzętu, oprogramowania i jego konserwację wyznaczonego przez Administratora Danych;
8. Użytkowniku – rozumie się osobę upoważnioną przez Administratora Danych do przetwarzania danych osobowych w systemie informatycznym oraz w kartotekach;
9. Pomieszczeniach – rozumie się prze to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego oraz gromadzone w kartotekach.

§ 4

1. Podstawowym celem zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych jest zapewnienie jak najwyższego standardu bezpieczeństwa tych danych. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, prze cały okres ich przetwarzania, charakteru poufnego wraz z zachowaniem ich integralności systemu informatycznego.
2. W celu zwiększenia efektywności ochrony danych osobowych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.
3. Zastosowane zabezpieczenia mają służyć osiągnięciu poniższych celów i zapewnić:
   1) poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
   2) integralność danych - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
   3) rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
   4) integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

§ 5

1. W celu uwzględnienia ewentualnych zagrożeń oraz kategorii przetwarzanych danych osobowych wprowadza się następujące poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym:
   1) podstawowy,
   2) podwyższony,
   3) wysoki.
2. Poziom co najmniej podstawowy stosuje się, gdy:
   1) w systemie informatycznym nie są przetwarzane dane osobowe,
   2) żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.
3. Poziom podwyższony stosuje się gdy:
   1) w systemie informatycznym są przetwarzane dane osobowe,
   2) żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.

4. Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służące do przetwarzania danych osobowych, połączone jest z siecią publiczną.
5. W systemach informatycznych Administratora Danych stosuje się poziom wysoki.

§ 6

1. Realizację zamierzeń określonych w § 4 powinny zagwarantować następujące założenia:
   1) wdrożenie procedur określających postępowanie osób dopuszczonych do przetwarzania danych osobowych oraz ich odpowiedzialność za ochronę tych danych,
   2) przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych,
   3) podpisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasło, identyfikatory) oraz zapewniający dostęp użytkowników do różnych poziomów zbiorów danych osobowych – stosownie do indywidualnego zakresu upoważnienia,
   4) podejmowanie niezbędnych działań w celu likwidacji stałych ogniw w systemie zabezpieczeń,
   5) okresowe sprawdzenie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych,
   6) opracowanie procedur odtworzenia systemu w przypadku wystąpienia awarii,
   7) śledzenie osiągnięć w dziedzinie zabezpieczenia systemów informacyjnych i – w miarę możliwości organizacyjnych i techniczno-finansowych – wdrożenie nowych narzędzi i metod pracy oraz sposobów zarządzania systemem informatycznym, które będą służyły wzmocnieniu bezpieczeństwa danych osobowych.
2. Przez politykę ochrony danych osobowych należy rozumieć określenie zadań, które należy realizować dla zapewnienia spójności wszystkich zabezpieczeń danych osobowych. Została on sformułowana w Polityce Ochrony Danych Osobowych oraz w kolejnych rozdziałach niniejszej Instrukcji. Odzwierciedla ona podstawowe zasady bezpieczeństwa, a także zarządzania systemem informatycznym oraz kartotekami u Administratora Danych.

ROZDZIAŁ II
Przydział uprawnień i identyfikatorów

§7

1. Każdy użytkownik dopuszczony do przetwarzania danych osobowych posiada stosowne upoważnienie. Wzór upoważnienia do przetwarzania danych osobowych. stanowi do Polityki Ochrony Danych Osobowych.
2. Każdy użytkownik posiada indywidualny identyfikator umożliwiający logowanie do tych aplikacji, z którymi może pracować.
3. Identyfikator umożliwia wykonywanie czynności zgodnie z zakresem powierzonych obowiązków, które wyznaczają poziom uprawnień.

4. Postanowienia ust. 2 nie dotyczą użytkowników, którzy przetwarzają wyłącznie dane osobowe gromadzone w kartotekach.
5. Prowadzona jest ewidencja przyznanych poszczególnym użytkownikom uprawnień związanych z dostępem do zbiorów danych oraz dokonywaniem zmian w zakresie przyznanych uprawnień.

§8

Każdy użytkownik systemu informatycznego przetwarzającego dane osobowe powinien posiadać umiejętność bezpiecznej obsługi komputera i dobrą znajomość oprogramowania systemowego i operacyjnego, z którego będzie korzystał.

§9

1. Każdy użytkownik - przed dopuszczeniem do obsługi systemu informatycznego, w którym przetwarzane są dane osobowe - podlega przeszkoleniu w zakresie:
   1) obsługi komputera, oprogramowania systemowego oraz oprogramowania do obsługi aplikacji, którą będzie wykorzystywał,
   2) przepisów o ochronie danych osobowych oraz wynikających z nich zadań oraz obowiązków.
2. Wszyscy użytkownicy podlegają okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (wymiana sprzętu na nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji.

§10

1. Za organizację szkoleń, o których mowa w § 9 ust. 1 pkt 1 odpowiedzialny jest ASI, zaś szkoleń, o których mowa w § 9 ust. 1 pkt 2 odpowiedzialny jest Inspektor Ochrony Danych Osobowych.

§11

Do uwierzytelniania użytkowników w systemie używa się haseł lub innych metod zapewniających weryfikację tożsamości użytkownika.

§12

Każdy użytkownik zobowiązany jest do zachowania w tajemnicy własnych haseł, także po upływie ich ważności.

§13

1. Identyfikatory dla użytkowników upoważnionych do przetwarzania danych osobowych w systemie informatycznym, niezbędne do logowania się do określonej aplikacji, ustala i przydziela ASI lub inna osoba upoważniona przez Administratora Danych.
2. Zakres uprawnień przypisany do identyfikatora przyznaje ASI na wniosek Administratora Danych.
3. Identyfikator użytkownika nie podlega zmianie.
4. Identyfikator użytkownika podlega rejestracji w systemie informatycznym.

§14

1. Pierwsze hasło dla użytkownika ustala ASI przy wprowadzaniu identyfikatora użytkownika do systemu.
2. Hasła muszą odpowiadać następującym wymogom:
   1) hasła składają się co najmniej z:
      a) dla poziomu bezpieczeństwa podstawowego 6 znaków,

b) dla poziomu bezpieczeństwa podwyższonego i wysokiego 8 znaków i powinny zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
2) nie mogą być zapisywane w systemie w postaci jawnej,
3) nie mogą być w nich używane imiona, nazwiska, przezwiska, inicjały i inne kombinacje znaków mogących doprowadzić do łatwego rozszyfrowania haseł przez osoby nieupoważnione,
4) nie mogą być w nich stosowane znaki następujące po sobie na klawiaturze bądź te same litery czy cyfry.

§15

1. Po otrzymaniu pierwszego hasła użytkownik zobowiązany jest zalogować się do systemu i powinien zmienić hasło. Przy wpisywaniu hasło nie może być wyświetlane na ekranie.
2. Hasło zmieniane jest nie rzadziej niż co 30 dni. Za systematyczną, terminową zmianę hasła odpowiada użytkownik.

§16

Hasło podlega natychmiastowej zmianie w przypadku podejrzenia jego odkrycia przez nieupoważnioną osobę.

§17

1. Hasła nie mogą być nigdzie zapisywane.
2. Tryb przechowywania i udostępniania haseł ASI określa załącznik nr 1 do niniejszej instrukcji.

ROZDZIAŁ III
Rejestrowanie i wyrejestrowywanie użytkowników

§18

1. Ewidencję osób upoważnionych do przetwarzania danych osobowych w zbiorach prowadzi osoba wyznaczona przez Administratora Danych. Wzór upoważnień do przetwarzania danych osobowych, stanowi załącznik nr 3 do Polityki Ochrony Danych Osobowych.

§19

Nośniki magnetyczne (optyczne), na których gromadzone są wykazy zawierające ewidencję użytkowników przechowywane są w wyznaczonych szafach lub sejfach, do których ma dostęp wyłącznie ASI lub osoba upoważniona przez Administratora Danych.

§20

Zmiany dotyczące użytkownika, takie jak:

1. zmiana imienia lub nazwiska,
2. zmiana zakresu upoważnienia,

podlegają niezwłocznemu odnotowaniu w ewidencji, o której mowa w § 18 Instrukcji.

§21

Zmiany dotyczące użytkownika, takie jak:

1. rozwiązanie umowy,
2. utrata upoważnienia do przetwarzania danych osobowych,
3. zmiana zakresu obowiązków służbowych skutkująca ustaniem upoważnienia,

powodują wyrejestrowanie użytkownika przez ASI, w trybie natychmiastowym, z ewidencji, o której mowa w § 18 Instrukcji, zablokowanie identyfikatora oraz unieważnienie hasła tego użytkownika.

§22

1. Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi.
2. Osoba prowadząca ewidencję, o której mowa w § 18 Instrukcji, obowiązana jest odrębnie gromadzić identyfikatory, które utraciły ważność lub też stosować odpowiednie ich oznaczenia.

§23

Dane dotyczące osób, które zostały wyrejestrowane z ewidencji osób upoważnionych do przetwarzania danych osobowych, z przyczyn, których mowa w § 21 ust. 1 Instrukcji. są gromadzone w postaci odrębnych zbiorów archiwalnych lub stosuje się odpowiednie ich oznaczenia.

ROZDZIAŁ IV
Procedury rozpoczęcia, zawieszenia i zakończenia pracy

§24

Przed przystąpieniem do pracy z systemem informatycznym lub kartotekami, użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz dokonać oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie poufności danych osobowych.

§25

W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie systemu, użytkownik obowiązany jest postępować zgodnie z zasadami określonymi w Polityce Ochrony Danych Osobowych.

§26

1. Rozpoczynając pracę na komputerze użytkownik loguje się do systemu informatycznego.
2. Użytkownik wprowadza identyfikator i dokonuje uwierzytelnienia.
3. Jeśli system to umożliwia, po przekroczeniu ustalonej liczby prób logowania system blokuje dostęp do systemu informatycznego na poziomie danego użytkownika.
4. ASI ustala przyczyny zablokowania systemu oraz w zależności od zaistniałej sytuacji podejmuje odpowiednie działania. O zaistniałym incydencie powiadamia Inspektora Ochrony Danych Osobowych lub osobę przez niego wyznaczoną.

§27

Przed opuszczeniem stanowiska pracy, użytkownik obowiązany jest:

1) wylogować się z systemu informatycznego lub,
2) poczekać, aż zaktywizuje się blokowany hasłem wygaszacz ekranu.

§28

Kończąc pracę należy:

1) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
2) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe, przed dostępem osób nieuprawnionych.

ROZDZIAŁ V
Procedury tworzenia kopii zapasowych

§29

1. Zbiory danych osobowych oraz programy i narzędzia programowe służące do ich przetwarzania, zapisywane na nośnikach zewnętrznych (streamer, dyski: wymienne, magnetyczne, optyczne) tworzące kopie zapasowe kolejnych okresów, powinny być odpowiednio oznakowane i przechowywane w wyznaczonych, odpowiednio zabezpieczonych pomieszczeniach.
2. Kopie zapasowe określone w ust. 1 powinny być sporządzane regularnie w okresach wyznaczonych w załączniku nr 2 do Instrukcji.
3. Za prawidłowe sporządzanie kopii zapasowych, ich oznakowanie i przechowywanie, odpowiedzialny jest ASI
4. Odpowiada on także za sprawdzanie poprawności wykonania kopii zapasowych na nośnik zewnętrzny.
5. Kopie zapasowe powinny być przechowywane w pomieszczeniu odrębnym od pomieszczeń, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.

§30

1. Użytkownicy obowiązani są przestrzegać terminów tworzenia doraźnych kopii zapasowych, o ile zostali do tego upoważnieni przez ASI.
2. Użytkownicy określeni w ust. 1 są odpowiedzialni za prawidłowe sporządzanie kopii zapasowych, ich oznakowanie i przechowywanie.

§31

1. Kopie zapasowe, które uległy uszkodzeniu lub ustała ich użyteczność podlegają natychmiastowemu zniszczeniu z zachowaniem procedur określonych niniejszą Instrukcją.
2. Zniszczenia kopii zapasowych, na nośnikach magnetycznych i optycznych dokonuje ASI w obecności Administratora Danych lub osoby przez niego wyznaczonej.
3. Z nośników magnetycznych i optycznych wielokrotnego użytku, np. CDRW dane należy usunąć w sposób uniemożliwiający ich odczytanie, a w przypadku, gdy usunięcie danych nie jest możliwe, nośniki podlegają zniszczeniu w stopniu uniemożliwiającym odzyskanie danych.
4. Dane zawarte na nośnikach optycznych jednokrotnego użytku, np. CDR należy usuwać poprzez całkowite zniszczenie nośnika.

ROZDZIAŁ VI
Przetwarzanie danych osobowych

§32

1. Dane osobowe przetwarzane są w kartotekach oraz w komputerach do tego przeznaczonych (serwerach, stacjach roboczych) zlokalizowanych w obszarach przetwarzania danych osobowych.
2. Kartoteki powinny być przechowywane w szafach, znajdujących się w wyznaczonych, odpowiednio zabezpieczonych, pomieszczeniach.
3. Wydruki robocze, błędne lub zdezaktualizowane powinny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowanie.
4. Opis obszaru przetwarzania danych osobowych oraz środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności danych osobowych określony jest w Polityce Ochrony Danych Osobowych.

§33

1. Kartoteka przekazywana jest do archiwum zgodnie z procedurami archiwizacji dokumentów.
2. Likwidacji zbiorów archiwalnych dokonuje się przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowanie.

§34

Decyzję o likwidacji zbiorów danych osobowych, przetwarzanych w kartotekach oraz systemach informatycznych podejmuje Administrator Danych.

§35

Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów danych osobowych. Inspektor Ochrony Danych Osobowych lub osoba przez niego upoważniona sporządza protokół, w którym zamieszcza następujące informacje:

1. datę dokonania likwidacji,
2. przedmiot likwidacji (nośniki, kartoteka),
3. przedział czasowy likwidowanych zbiorów danych osobowych,
4. podpisy osób dokonujących i obecnych przy likwidacji zbiorów danych osobowych.

ROZDZIAŁ VII
Zabezpieczenie systemu informatycznego

§36

System informatyczny zabezpiecza się przed:

1. działaniem, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
2. utratą danych spowodowaną:
   a) działaniem nieautoryzowanego oprogramowania.
   b) awarią zasilania lub zakłóceniami w sieci zasilającej.

§37

1. ASI odpowiada za niezwłoczne instalowanie na sprzęcie najnowszych wersji oprogramowania zabezpieczającego system informatyczny.
2. Nowe wersje oprogramowania instaluje wyłącznie ASI niezwłocznie po ich otrzymaniu lub osoba upoważniona przez ASI.

3. Okresowych kontroli w zakresie instalowania najnowszych wersji oprogramowania zabezpieczającego system informatyczny dokonuje Inspektor Ochrony Danych Osobowych lub osoba przez niego upoważniona.

§38

1. Na serwerach i stacjach roboczych używanych przez Administratora Danych powinno instalować się przynajmniej jeden program antywirusowy.
2. Program antywirusowy należy instalować również na komputerach przenośnych.

§39

W komputerach przenośnych zawierających dane osobowe stosuje się środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

§40

1. Kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie informatycznym, jak i do celów instalacyjnych.
2. Na serwerach, w miarę możliwości technicznych, oprogramowanie antywirusowe powinno być aktywne cały czas.
3. Na stacjach roboczych oprogramowanie antywirusowe powinno być aktywne cały czas i powinno dokonywać sprawdzenia każdego otwieranego lub uruchomianego pliku.

§41

Użytkownicy są zobowiązani do dokonywania kontroli antywirusowej wszystkich nośników magnetycznych lub optycznych przychodzących z zewnątrz oraz okresowo nośników własnych.

§42

1. W razie stwierdzenia zainfekowania systemu, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie ASI.
2. ASI usuwa wirusa, jeśli automatycznie nie dokonał tego program antywirusowy oraz informuje Inspektora Ochrony Danych Osobowych lub osobę przez niego upoważnioną o dokonanych czynnościach i rodzaju wirusa.

§43

W razie niemożności usunięcia wirusa, ASI za zgodą Inspektora Ochrony Danych Osobowych, korzysta z usług zewnętrznych specjalistów w tej dziedzinie.

§44

1. W sytuacji korzystania z usług zewnętrznych specjalistów, należy podjąć działania uniemożliwiające tym osobom dostęp do danych osobowych.
2. Prace określone w ust. 1 są wykonywane pod nadzorem ASI lub upoważnionego użytkownika i w miarę możliwości bez dostępu do danych osobowych.

§45

1. ASI jest odpowiedzialny za kontrolę antywirusową serwerów i zasobów sieciowych.
2. Użytkownicy są odpowiedzialni za kontrolę antywirusową na dyskach lokalnych i używanych nośnikach danych.

§46

1. Po usunięciu wirusa ASI sprawdza zainfekowany system informatyczny oraz przywraca go do pełnej sprawności i funkcjonalności.
2. ASI sporządza raport o wystąpieniu wirusa. Raport winien zawierać następujące informacje:
   1) nazwę wirusa,
   2) datę wykrycia wirusa,
   3) miejsce zainfekowania,
   4) źródło infekcji.
3. Raport, o którym mowa w ust. 2 przekazywany jest Inspektorowi Ochrony Danych Osobowych lub osobie przez niego wyznaczonej wraz z wnioskami, stosownymi do zaistniałej sytuacji.

§47

1. Przy przetwarzaniu danych osobowych zakwalifikowanych do poziomu bezpieczeństwa wysokiego system informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
2. W przypadku zastosowania logicznych zabezpieczeń, o których mowa w ust. I, obejmują one:
   1) kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną,
   2) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.
3. Wobec danych wykorzystywanych do uwierzytelniania, które są przesyłane w sieci publicznej stosuje się środki ochrony kryptograficznej.

§48

ASI prowadzi wykaz przypadków zainfekowania komputerów i nośników wykorzystywanych do przetwarzania danych osobowych w systemie oraz przechowuje kopie raportów.

§49

Procedura wyrażona w niniejszym rozdziale ma zastosowanie także do przypadków awarii systemu spowodowanych błędem programu bądź użytkownika.

ROZDZIAŁ VIII
Wymagania dotyczące sprzętu i oprogramowania

§50

1. Sprzęt obsługujący zbiór danych osobowych składa się z komputerów stacjonarnych klasy PC.
2. Komputery przenośne mogą być używane do przetwarzania danych osobowych po odpowiednim ich zabezpieczeniu.
3. Użytkownik korzystający z komputera przenośnego jest zobowiązany do zachowania szczególnej ostrożności podczas transportu komputera oraz nie może udostępnić komputera osobom nieupoważnionym.
4. Szczegółowy wykaz sprzętu i oprogramowania wykorzystywanego do przetwarzania danych osobowych znajduje się w dokumentacji księgowej.

§51

Sieć komputerowa służąca do przetwarzania danych osobowych powinna mieć zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu komputerowego.

§52

1. Za prawidłowe zasilanie energetyczne sieci komputerowej odpowiedzialny jest ASI.
2. Infrastruktura techniczna związana z siecią komputerową i jej zasilaniem (rozdzielnie elektryczne, skrzynki z bezpiecznikami) powinna być zabezpieczona przed dostępem osób nieupoważnionych.

§53

1. Dane osobowe przesyłane na nośnikach magnetycznych i optycznych oraz za pomocą systemów teleinformatycznych powinny być zabezpieczone w sposób uniemożliwiający dostęp do nich osób nieupoważnionych.
2. Dane osobowe przesyłane po łączach telekomunikacyjnych wewnątrz danej sieci powinny być dodatkowo zabezpieczone w sposób uniemożliwiający dostęp do danej sieci LAN z innej sieci.
3. Dane osobowe przesyłane po łączach telekomunikacyjnych na zewnętrz powinny być w miarę możliwości technicznych szyfrowane za pomocą algorytmu kryptograficznego.

§54

Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych muszą być użytkowane z zachowaniem praw autorskich i posiadać licencje.

§55

1. ASI odpowiada za wyposażenie systemu informatycznego w mechanizmy uwierzytelniania użytkownika oraz za sprawowanie kontroli dostępu do danych osobowych jedynie osób upoważnionych.
2. System informatyczny wykorzystywany przez użytkowników wyłącznie w celach służbowych. Wyjątki od powyższej reguły możliwe są jedynie za wyraźna zgodą Administratora Danych.
3. System informatyczny może być monitorowany, w tym również z zastosowaniem specjalistycznego oprogramowania lub sprzętu, w celu rejestracji aktywności użytkowników oraz sposobu wykorzystywania systemu informatycznego przez użytkowników.

§56

1. Ekrany monitorów powinny być w miarę możliwości wyposażone w wygaszacze zabezpieczone hasłem, które aktywują się automatycznie po upływie określonego czasu od ostatniego użycia komputera.
2. Ekrany monitorów, powinny być ustawione w taki sposób, żeby w miarę możliwości uniemożliwić odczyt wyświetlanych informacji osobom nieupoważnionym.
3. Za spełnienie obowiązku określonego w ust. 2 odpowiadają użytkownicy.

§57

1. ASI jest odpowiedzialny za to, aby dla każdej osoby, której dane osobowe są przetwarzane, system informatyczny zapewniał odnotowanie:
   1) daty pierwszego wprowadzenia danych do systemu,

2) identyfikatora użytkownika wprowadzającego dane, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba,
3) źródła danych, w przypadku zbierania danych nie od osoby, której one dotyczą,
4) informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych,
5) sprzeciwu,

Wymagania określone w niniejszym ustępie nie dotyczą systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie.

1. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzania danych.
2. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.
3. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.
4. Do czasu spełnienia przez system informatyczny wszystkich wyżej wymienionych wymogów, system informatyczny powinien zapewnić odnotowanie:
   1) daty pierwszego wprowadzenia danych,
   2) identyfikatora użytkownika wprowadzającego dane, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba.
5. Do chwili spełnienia przez system informatyczny wszystkich wymogów określonych w niniejszym paragrafie, odnotowanie informacji określonych w ust. 1 pkt 3, 4 i 5 należy prowadzić w formie tradycyjnej (papierowej) lub komputerowo poza systemem.

ROZDZIAŁ IX
Procedury wykonywania przeglądów i konserwacji

§58

1. Bieżących oraz okresowych przeglądów, napraw i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych, niewymagających angażowania zewnętrznych firm serwisowych, dokonuje ASI.
2. Przeglądów i konserwacji zbiorów danych osobowych dokonują użytkownicy, zgodnie z indywidualnymi zakresami upoważnień i odpowiedzialności.

§59

Prace dotyczące przeglądów, konserwacji i napraw, wymagające zaangażowania firm zewnętrznych, są wykonywane za wiedzą Inspektora Ochrony Danych Osobowych przez uprawnionych przedstawicieli tych firm pod nadzorem ASI lub upoważnionego użytkownika i w miarę możliwości bez dostępu do rzeczywistych danych osobowych.

§60

1. W przypadku, gdy zaistnieje potrzeba naprawy lub wymiany sprzętu komputerowego służącego do przetwarzania lub przechowywania danych osobowych należy usunąć dane, w sposób uniemożliwiający ich odzyskanie.
2. Jeżeli nie ma możliwości usunięcia danych należy urządzenie uszkodzić w sposób uniemożliwiający ich odczytanie.

§61

Nadzór nad instalowaniem, sprawnym funkcjonowaniem i wymianą uszkodzonych urządzeń oraz ich likwidacją sprawuje ASI lub osoba wyznaczona przez Administratora Danych.

ROZDZIAŁ X
Postanowienia końcowe

§62

Instrukcja jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.

§63

1. Użytkownik zobowiązany jest złożyć oświadczenie, o tym, iż został zaznajomiony z przepisami ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych oraz dokumentacją obowiązującą u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania.
2. Oświadczenia przechowywane są w aktach osobowych.

§64

1. W sprawach nieuregulowanych w niniejszej Instrukcji mają zastosowanie przepisy ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych.
2. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Instrukcji.

…….
(podpis Administratora Danych)

Załącznik nr 1 do Instrukcji
zarządzania systemem
informatycznym

TRYB PRZECHOWYWANIA I UDOSTĘPNIANIA HASEŁ ASI

Ustala się następujący tryb postępowania z hasłami ASI:

1. Hasła ASI przechowywane są w formie pisemnej w zapieczętowanej kopercie.
2. Koperta złożona jest w specjalnej szafie, do której dostęp posiada wyłącznie Administrator i osoby przez niego upoważnione.
3. Hasła* o którym mowa w pkt 1 dają najwyższe uprawnienia administratorskie do korzystania i obsługi systemu informatycznego.
4. Hasła zmieniane są co najmniej co 30 dni bądź natychmiast w przypadku podejrzenia odkrycia przez inną, nieupoważnioną osobę.
5. Nowe, aktualne hasło zabezpiecza się według procedur opisanych w pkt I i 2.
6. Koperta wraz z hasłem, które straciło ważność podlega zniszczeniu przy użyciu niszczarki dokumentów.
7. Niszczenia, o którym mowa w pkt 6 dokonuje ASI w obecności Administratora Danych lub osoby przez niego upoważnionej.
8. W sytuacjach awaryjnych zaistniałych pod nieobecność ASI lub w razie jego niedyspozycji Administrator Danych udostępnia hasło osobie przez siebie wyznaczonej.

(podpis Administratora Danych)

Załącznik nr 2 do Instrukcji zarządzania
systemem informatycznym

CZĘSTOTLIWOŚĆ TWORZENIA KOPII ZAPASOWYCH

Ustala się następującą częstotliwość tworzenia kopii awaryjnych:

1. Kopie dobowe i tygodniowe, wykonywane przez ASI lub użytkowników obejmujące:
    a. serwery danych,
    b. dział finansowy.
2. Kopie miesięczne, wykonywane na nośnikach zewnętrznych - magnetycznych lub optycznych umieszczane w zapieczętowanych kopertach, deponowane przez ASI w miejscu określonym w § 29 Instrukcji obejmujące:
        i. serwery danych,
        ii. dział finansowy,
        iii. stacje robocze.
3. Kopie tygodniowe przechowywane są do czasu zdeponowania kopii miesięcznych.
4. Niszczenie kopii awaryjnych należy wykonywać w sposób określony w Instrukcji.
5. W sytuacjach awaryjnych zaistniałych pod nieobecność ASI lub w razie jego niedyspozycji Dyrektora udostępnia kopie awaryjne osobie przez siebie wyznaczonej.

(podpis Administratora Danych)

00-682 Warszawa, ul. Hoża 86/ 410; 62-200 Gniezno ul. Platanowa nr 15
61-806 Poznań, ul. Święty Marcin 29/8; konto nr 45 1940 1076 3105 0557 0000 0000
KRS 0000 406 825; NIP: 784-248-78-16; Regon: 302 011 576
www.lesny.com.pl; kancelaria@lesny.com.pl