Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych

Okręg Mazowiecki
Polskiego Związku Wędkarskiego
w Warszawie

I. Podstawowe definicje

1. Administrator Danych – Okręg Mazowiecki Polskiego Związku Wędkarskiego w Warszawie (dalej zwany Administrator lub OMPZW) decydujący o celach i środkach przetwarzania danych osobowych;
2. Administrator systemu informatycznego (ASI) - wyznaczona przez ADO osoba nadzorującą pracę systemu informatycznego oraz wykonująca w nim czynności wymagające najwyższych uprawnień;
3. Rozporządzeniu – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z dnia 29 kwietnia 2004 r. (Dz.U. Nr 100, poz. 1024);
4. Ustawie – rozumie się przez to ustawę z dnia z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922 ze zm.);
5. Dane osobowe (dane) - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczna, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu i działań. Danymi osobowymi będą, zatem zarówno takie dane, które pozwalają na określenie tożsamości konkretnej osoby, jak i takie, które nie pozwalają na jej natychmiastową identyfikację, ale są przy pewnym nakładzie kosztów, czasu i działań, wystarczające do jej ustalenia;
6. Dane wrażliwe – dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym;

7. Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi, zapewniający mu dostęp do danych osobowych przetwarzanych w systemie informatycznym;
8. Identyfikator – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
9. Instrukcja – niniejsza Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, która została przyjęta jako obowiązujący dokument w OMPZW;
10. Integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
11. Integralność systemu – właściwość zapewniająca nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
12. Nośnik danych – nośnik służący do zapisu i przechowywania informacji, np. taśmy, płyty, dyski twarde;
13. Odbiorca danych – każdy, komu udostępnia się dane osobowe, z wyłączeniem: osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, przedstawiciela podmiotu przetwarzającego dane osobowe mającego siedzibę lub miejsce zamieszkania w państwie trzecim, podmiotu, któremu powierzono przetwarzanie danych osobowych, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;
14. Pracownik - osobę zatrudnioną na podstawie stosunku pracy lub umowy cywilno-prawnej;
15. Poufność danych – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom;
16. Przetwarzanie danych – 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;
17. Rozliczalność – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

18. System informatyczny – sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, zasad przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
19. Usuwanie danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
20. Użytkownik – osoba upoważniona, której ASI nadał upoważnienie i przyznał hasło;
21. Zabezpieczenie systemu informatycznego – należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą;
22. Zbiór danych/baza danych osobowych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

II. Postanowienia ogólne

1. Niniejsza Instrukcja stanowi Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych, o której mowa w Rozporządzeniu 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).

2. Osobami zobowiązanymi do przestrzegania niniejszej Instrukcji są wszyscy Użytkownicy Systemów informatycznych posiadający nadane uprawnienia do tych Systemów.

3. Z uwagi na fakt, iż urządzenia końcowe służące do przetwarzania danych osobowych połączone są z siecią Internet, OMZWP zapewnia wysoki stopień bezpieczeństwa danych osobowych, o którym mowa w § 6 Rozporządzenia.

III. Uprawnienia i odpowiedzialności

1. Administrator danych

1) Administrator Danych wprowadza niniejszą Instrukcję i nadzoruje wdrożenie procesów administrowania i zarządzania środkami informatycznymi wspomagającymi procesy przetwarzania informacji stanowiących dane osobowe.

2) Stwarza właściwe warunki organizacyjno-techniczne gwarantujące bezpieczeństwo systemów informatycznych, w szczególności:

3) Zabezpiecza pomieszczenia, w których przetwarzane są dane osobowe w systemach informatycznych przed dostępem osób niepowołanych.

4) Odpowiada za zapoznanie pracownika z zasadami Instrukcji ochrony danych osobowych i Instrukcji zarządzania systemem informatycznym oraz z zakresem kompetencji i odpowiedzialności związanych z dostępem do danych,

5) Administrator danych odpowiada za aktualizację niniejszej Instrukcji w przypadku zmian w przepisach prawnych, zmian organizacyjno-funkcjonalnych oraz aktualizuje stosownie do zmieniających się technologii informatycznych oraz zagrożeń bezpieczeństwa systemów informatycznych,

6) sprawuje nadzór nad zapewnieniem awaryjnego zasilania elementów systemu informatycznego oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
7) sprawuje nadzór nad naprawami, konserwacją oraz likwidacją urządzeń teleinformatycznych, na których zapisane są dane osobowe,
8) identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych,
9) określa potrzeby w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe,
10) monitoruje działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych,
11) sprawuje nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane oraz kontrolę dostępu do danych,

2. Administrator systemów informatycznych:

1) konfiguruje infrastrukturę informatyczną zgodnie z wymaganiami bezpieczeństwa i zaleceniami producenta,
2) nadaje unikalne identyfikatory i uprawnienia dostępu użytkownikom systemu,
3) kontroluje prawidłowość wykorzystania systemu przez użytkowników (zgodnie z obowiązującą dokumentacją i procedurami eksploatacyjnymi),
4) dokonuje wyboru lub migracji do technologii minimalizującej zagrożenie uzyskania dostępu do sieci osobom nieupoważnionym,
5) wykonuje przeglądy techniczne oraz bieżące konserwacje infrastruktury informatycznej niezbędnej do funkcjonowania systemu,
6) nadzoruje proces monitorowania sieci pod kątem zabezpieczenia przed dostępem osób nieupoważnionych,
7) dokonuje zakupu pamięci masowych oraz innych urządzeń i nośników umożliwiających wykonywanie kopii zapasowych danych osobowych w systemach informatycznych,
8) zgłasza potrzebę zakupu systemów operacyjnych, oprogramowania antywirusowego oraz systemów kryptograficznych podnoszących bezpieczeństwo danych osobowych, gwarantujących spełnienie wymogów określonych ustawą,

9) konfiguruje i parametryzuje urządzenia sieciowe zgodnie z wymaganiami bezpieczeństwa i zaleceniami producenta,
10) dokonuje właściwego prowadzenia i zabezpieczenia okablowania sieci komputerowej służącej do przetwarzania danych osobowych w systemach informatycznych w celu wyeliminowania zagrożeń.

3. Użytkownik systemu zobowiązany jest:

1) Zapoznania się i przestrzegania Instrukcji zarządzania systemem informatycznym,
2) Utrzymania właściwego poziomu bezpieczeństwa na swoim stanowisku pracy,
3) Obsługi systemu i infrastruktury informatycznej zgodnie z wymaganiami bezpieczeństwa i procedurami eksploatacyjnymi,
4) Zachowania poufności danych, do których uzyskał dostęp z wykorzystaniem systemu informatycznego,
5) Zapewnienia zgodności i poprawności danych wprowadzanych do systemu,
6) Udziału w szkoleniach z zakresu bezpieczeństwa,
7) Zgłaszania wszelkich zdarzeń, które naruszają lub mogą naruszyć zasady Instrukcji zarządzania systemem informatycznym a także informacji o zauważonych zagrożeniach mogących wpłynąć na bezpieczeństwo.

IV. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Systemy informatyczne przetwarzające dane osobowe są wyposażone w mechanizmy uwierzytelniania Użytkowników oraz kontroli dostępu do tych danych.
2. Dla każdego Użytkownika systemu informatycznego, w którym przetwarza się dane osobowe, ustalony jest odrębny identyfikator oraz hasło. Login oraz hasło mają charakter poufny. Zabronione jest udostępnianie swojego hasła osobom trzecim.
3. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym Użytkownik uzyskuje wyłącznie po uwierzytelnieniu przy użyciu swojego loginu oraz hasła.
4. Po nadaniu hasła inicjacyjnego Użytkownik jest zobowiązany do jego zmiany przy pierwszym logowaniu do systemu.
5. Hasło musi się składać z co najmniej 8 znaków, zawierać co najmniej jedną dużą literę i co najmniej jedną cyfrę lub znak specjalny.
6. Hasło nie może być tożsame z jednym z pięciu ostatnio ustanowionych haseł.
7. Ilość prób w przypadku błędnego wprowadzenia hasła jest ograniczona do liczby 3 (trzech) i skutkuje blokadą systemu na 30 (trzydzieści) minut. Odblokowanie Systemu jest możliwe przez ASI.
8. Hasło nie może zawierać cyfr, liter i oznaczeń zbieżnych z osobistymi danymi użytkownika, takimi jak np.: imię, nazwisko, data urodzenia użytkownika, imiona i nazwiska osób bliskich użytkownikowi, numery telefonów, pin, kody kart płatniczych, numer PESEL, numer dokumentów osobistych itp.).
9. System wymusza okresową zmianę hasła nie rzadziej, niż co 30 (trzydzieści) dni.
10. W przypadku systemów, w których ze względów technicznych nie jest możliwe ustawienie systemowego wymuszania okresowej zmiany hasła, każdy Użytkownik zobowiązany jest we własnym zakresie dbać o jego zmianę, z częstotliwością nie rzadziej, niż co 30 (trzydzieści) dni.
11. Hasła wpisywane z klawiatury komputera nie mogą pojawiać się na ekranie monitora w formie jawnej.

12. Pracownik traci uprawnienia dostępu do danych osobowych w przypadku rozwiązania umowy, urlopu macierzyńskiego, urlopu wychowawczego, urlopu bezpłatnego lub zwolnienia lekarskiego powyżej 30 dni.
13. Administrator dokonuje zmiany w Ewidencji Użytkowników. Identyfikator Użytkownika, który utracił prawo dostępu do systemu Informatycznego, nie może być przydzielony innej osobie.
14. Hasła administratora ASI przekazuje Administratorowi.

V. Procedura nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

1. Dostęp do zasobów systemów ograniczony jest do zakresu niezbędnego dla wypełniania obowiązków służbowych i realizacji uprawnień związanych z pełnioną funkcją.
2. Za nadawanie identyfikatorów w systemie informatycznym odpowiada ASI. Ewidencję prowadzi upoważniona przez Administratora osoba.
3. Nadawanie oraz zmiana uprawnień w systemie informatycznym odbywa się na podstawie formularza zatwierdzonego przez Administratora.
4. Uprawnienia są odbierane przez ASI, na wniosek Administratora. Po odebraniu uprawnień Identyfikator Użytkownika nie może zostać przydzielony innemu Użytkownikowi.

VI. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla Użytkowników systemu

1. Przed przystąpieniem do pracy każdy Użytkownik zobowiązany jest:
   1) sprawdzić stację roboczą oraz jej otoczenie ze zwróceniem uwagi, czy nie zachodzą okoliczności wskazujące na naruszenie ochrony informacji w tym danych osobowych;

2) zapewnić poufne warunki pracy, m.in. poprzez ustawienie monitora w sposób uniemożliwiający wgląd w informacje wyświetlane na monitorze.

2. W przypadku podejrzenia incydentu bezpieczeństwa (np. uszkodzenie stacji roboczej, brak dostępu do zasobów po zalogowaniu się do systemu informatycznego) Użytkownik zobowiązany jest niezwłocznie skontaktować się z ASI lub Administratorem.

3. Rozpoczęcie pracy w Systemie Informatycznym możliwe jest po uprzednim zalogowaniu się przez Użytkownika przy użyciu jego identyfikatora i hasła.

4. Przed każdorazowym opuszczeniem stanowiska pracy Użytkownik zobowiązany jest zablokować stację roboczą przed dostępem osób postronnych poprzez jednoczesne naciśnięcie klawisz [windows] + L lub ctrl+alt+del i zatwierdzenie klawiszem Enter (dot. systemów Windows). W przypadku innych systemów operacyjnych – zgodnie z wymaganiami dla tych systemów.

5. W przypadku upływu 15 (piętnastu) minut nieaktywności Użytkownika, system włącza automatyczną blokadę dostępu do stacji roboczej.

6. Przed zakończeniem pracy w systemie Użytkownik zobowiązany jest zamknąć w bezpieczny sposób wszystkie systemy oraz aplikacje t.j. poprzez wylogowanie się, a następnie wyłączyć stację roboczą, wykorzystując w tym celu dedykowane funkcje systemu operacyjnego. Użytkownik zobowiązany jest pozostać przy stanowisku pracy do czasu, aż proces zamykania Systemu operacyjnego zostanie ukończony.

VII. Procedury tworzenia kopii zapasowych zbiorów danych, programów i narzędzi programowych służących do ich przetwarzania oraz sposób, miejsce i okres przechowywania elektronicznych nośników zawierających dane osobowe oraz kopii zapasowych

1. W celu zabezpieczenia danych osobowych przed ich zmianą, utratą, uszkodzeniem lub zniszczeniem wykonuje się ich kopie zapasowe.
2. Tworzenie kopii zapasowych zbiorów danych osobowych:

3. Program Symfonia - pełna kopia wykonywana codziennie przechowywana na zapasowym serwerze
4. Pozostałe kopie wykonywane zgodnie z umowami powierzenia.

2. Administrator Systemu Informatycznego odpowiedzialny za tworzenie kopii zapasowych zobowiązany jest przestrzegać terminów sporządzania kopii zapasowych oraz raz w roku dokonywać kontroli możliwości odtworzenia danych zapisanych na tych kopiach pod kątem ewentualnej przydatności w sytuacji awarii systemu. Z testowania poprawności zapisu i możliwości odtworzenia danych z kopii zapasowych sporządzane są zapisy.
3. Nośniki z kopiami zapasowymi przechowywane są w innym miejscu, niż to w którym dane osobowe są przetwarzane na bieżąco. Nośniki z kopiami zapasowymi przekazywane są do miejsca docelowego w sposób zapewniający ich bezpieczeństwo.
4. ASI przeprowadza okresowe, cykliczne testy odtworzeniowe Systemu z kopii zapasowej. Z każdego testu sporządzany jest szczegółowy raport, będący podstawą podjęcia decyzji co do ewentualnych działań naprawczych.

VIII. Korzystanie z oprogramowania

1. Każde oprogramowanie dopuszczone do pracy ma autoryzację Administratora Systemów Informatycznych do użytkowania w infrastrukturze informatycznej.
2. Nieautoryzowane oprogramowanie jest niezwłocznie usuwane, a przypadki takie są przedmiotem postępowań wyjaśniających i dyscyplinujących.
3. Zabronione jest użytkowanie własnego i nielicencjonowanego oprogramowania.
4. Administrator Systemów Informatycznych odpowiada za utrzymywanie rejestru zasobów i kontrolę zmian oprogramowania wykorzystywanego w OMPZW.
5. Rejestr zasobów zawiera w szczególności: nazwę oprogramowania, typ systemu, miejsce instalacji (lokalizacja), opis/ funkcję oraz informację o warunkach licencji (ograniczenia, liczba użytkowników).
6. Przeprowadzane są okresowe kontrole legalności oprogramowania oraz zgodności wykorzystania z postanowieniami umów licencyjnych.

IX. Przechowywanie nośników informacji zawierających dane osobowe

1. Zabezpieczenie elektronicznych nośników informacji

   1) Nośniki danych są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych).

   2) Zabrania się wynoszenia poza obszar OMPZW wymiennych nośników informacji a w szczególności twardych dysków z zapisanymi danymi osobowymi bez zgody Administratora.

   3) Użytkownicy są zobowiązani do niezwłocznego i trwałego usuwania/kasowania danych osobowych z nośników informacji po ustaniu powodu ich przechowywania (chyba, że z powodu odrębnych przepisów należy je zachować na dłużej).

   4) Podlegające likwidacji uszkodzone lub przestarzałe nośniki a szczególności twarde dyski z danymi osobowymi są komisyjnie niszczone w sposób fizyczny, co znajduje odzwierciedlenie w Protokole zniszczenia uszkodzonych nośników.

   5) Nośniki informacji zamontowane w sprzęcie IT, a w szczególności twarde dyski z danymi osobowymi powinny być wymontowane lub wyczyszczone specjalistycznym oprogramowaniem, zanim zostaną przekazane poza obszar OMPZW np. sprzedaż lub naprawa).

2. Zabezpieczenie dokumentów i wydruków

   1) Dokumenty i wydruki trwałe z danymi osobowymi przechowuje się w archiwum lub w zabezpieczonych fizycznie pomieszczeniach, biurkach i szafach.

   2) Pracownicy są zobowiązani do zabezpieczania dokumentów (np. zamykanie dokumentów na klucz w szafach, biurkach) przed dostępem osób nieupoważnionych podczas swojej nieobecności w pomieszczeniach lub po zakończeniu pracy (tzw. Polityka czystego biurka).

   3) Zabrania się pozostawiania wydruków oraz ksero na drukarkach, skanerach i kserokopiarkach bez nadzoru.

   4) Pracownicy są zobowiązani do niszczenia dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania

X. Procedura zabezpieczenia systemu informatycznego, w tym przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. Ochrona antywirusowa

    1) Celem procedury jest zabezpieczenie systemów informatycznych przed szkodliwym oprogramowaniem (np. typu robaki, wirusy, konie trojańskie, rootkity) oraz nieautoryzowanym dostępem do systemów przetwarzających dane osobowe.

    2) W celu zabezpieczenia zasobów informatycznych wykorzystywane jest oprogramowanie antywirusowe Kasperski

    3) Za zaplanowanie i zapewnienie ochrony antywirusowej odpowiada ASI, w tym za zapewnienie odpowiedniej liczby licencji dla użytkowników.

    4) Użytkownicy zobowiązani są do skanowania plików programem antywirusowym.

    5) ASI zapewnia stałą aktywność programu antywirusowego. Tzn. program antywirusowy musi być aktywny podczas pracy systemu informatycznego przetwarzającego dane osobowe.

    6) W przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik powinien niezwłocznie powiadomić o tym fakcie ASI.

2. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej

    1. Stosowane zabezpieczenia mają na celu zabezpieczenie systemów informatycznych przed nieautoryzowanym dostępem do sieci lokalnej np. przez programy szpiegujące, hackerów.

    2. Za zaplanowanie, konfigurowanie, aktywowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku sieci lokalnej i sieci rozległej odpowiada ASI.

    3. Stosowany jest Firewall na serwerze.

    4. Sieć bezprzewodową zabezpieczono za pomocą standardu szyfrowania WPA.

XI. Zasady i sposób odnotowywania w systemie informacji o udostępnianiu danych osobowych

1. System przetwarzający dane osobowe udostępniane odbiorcom musi umożliwiać rejestrację:
    1. nazwy jednostki organizacyjnej lub imienia i nazwiska osoby, której udostępniono dane,
    2. zakresu udostępnianych danych,
    3. daty udostępnienia.
2. Dane osobowe udostępnia się Odbiorcy danych na pisemny wniosek ze wskazaniem przez Odbiorcę podstawy prawnej legalizującej przetwarzanie danych osobowych, z art. 23 lub art. 27 Ustawy.
3. Zgody na udostępnienie danych udziela Administrator .
4. Odnotowanie informacji o udostępnieniu danych powinno nastąpić niezwłocznie po udostępnieniu danych: w systemie informatycznym, jeśli przetwarza udostępnione dane osobowe lub w postaci rejestru udostępniania danych osobowych, której wzór stanowi Załącznik 08 do Polityki.
5. Administrator odpowiada za udostępnienie danych osobowych w sposób zgodny z ich przeznaczeniem.
6. Na żądanie osoby, której dane zostały udostępnione, informacje o udostępnieniu danych są zamieszczane w raporcie z systemu informatycznego lub wyciągu z rejestru papierowego, a raport przekazywany jest tej osobie.

XII. Procedura wykonywania przeglądów i konserwacji

1. Celem procedury jest zapewnienie ciągłości działania systemów informatycznych przetwarzających dane osobowe oraz zabezpieczenie danych osobowych przed ich nieuprawnionym udostępnieniem.
2. Przeglądy i konserwacje systemu informatycznego i aplikacji.
3. ASI odpowiada za bezawaryjną i poprawną pracę systemu informatycznego, w tym: stacji roboczych, aplikacji serwerowych, baz danych, poczty e-mail.

4. Przegląd i konserwacja systemu informatycznego powinny być wykonywane w terminach określonych przez producentów systemu lub zgodnie z harmonogramem ASI, jednak nie rzadziej, niż raz w roku.
5. Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI.
6. ASI odpowiada za optymalizację zasobów serwerowych, wielkości pamięci i dysków.
7. ASI odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia.
8. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego, wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.
9. Czynności konserwacyjne i naprawcze wykonywane doraźnie przez osoby nie posiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych), muszą być wykonywane pod nadzorem osób upoważnionych.
10. Przed przekazaniem uszkodzonego sprzętu komputerowego z danymi osobowymi do naprawy poza fizyczny obszar przetwarzania OMPZW należy:
    a) wymontować nośniki z danymi osobowymi,
    b) trwale usunąć dane osobowe z użyciem specjalistycznego oprogramowania,
    c) podpisać umowę powierzenia z podmiotem wykonującym naprawę, jeżeli nie ma możliwości trwałego usunięcia danych lub trwałe usunięcie danych z innych przyczyn nie jest możliwe.
11. Monitorowanie systemów i infrastruktury informatycznej

XIII. Systemy i infrastruktura informatyczna podlegają monitorowaniu przez Administratora Systemów Informatycznych.

1. W szczególności monitorowaniu i rejestrowaniu podlegają:
    a) nieudane próby logowania do systemu,
    b) błędy systemu,

c) zmiany w plikach konfiguracyjnych i krytycznych zmiennych systemowych,

d) wersje systemu i stan uaktualnień,

e) obciążenie procesorów, zajętość pamięci dyskowej i operacyjnej,

f) ruch sieciowy i przesyłane dane,

g) dziennik zagrożeń systemu antywirusowego.

h) Kompletne rejestry zdarzeń są przechowywane co najmniej przez miesiąc.

XIV. W celu wykrywania incydentów związanych z bezpieczeństwem Administrator Systemów Informatycznych regularnie, nie rzadziej niż raz na miesiąc, monitoruje zapisy dokonywane automatycznie przez systemy w rejestrach zdarzeń pod kątem właściwego wykorzystania systemu teleinformatycznego i zarządzania nim.

1. Ruch sieciowy i przesyłane dane mogą być blokowane w przypadku, gdy naruszają przepisy prawa lub zasady obowiązującej dokumentacji.
2. Administrator Systemów Informatycznych prowadzi dziennik wykonywanych czynności oraz zdarzeń zachodzących w systemie.
3. Dziennik pracy systemu składa się z ewidencji zawierających zapisy dotyczące następujących zdarzeń lub czynności:

a) informacje o tworzonych nowych identyfikatorach oraz prawach im przypisanych, ich modyfikowaniu i usuwaniu,

b) informacje o sesjach połączeń zdalnych wykonywanych przez strony trzecie,

c) ewidencji oprogramowania dopuszczonego do pracy również aktualizacje oprogramowania,

d) aktualizacje bazy sygnatur programu antywirusowego,

e) błędy systemowe,

f) konfiguracja sprzętu i systemu operacyjnego,

g) ewidencji wymiennych nośników komputerowych,

h) incydenty związane z naruszeniem systemu ochrony.

2. Ochrona antywirusowa

    1. Stacje robocze i serwery objęte są ochroną przed naruszeniem integralności danych, wykonywaną w czasie rzeczywistym, za pomocą oprogramowania antywirusowego.
    2. Każdy nośnik danych dostarczony do OMPZW powinien być przed użyciem bezwzględnie skontrolowany aktualnym oprogramowaniem antywirusowym.
    3. Kontrola systemów informatycznych pod kątem obecności złośliwego oprogramowania, jest realizowana przez ASI.

3. Zgłaszanie błędów / awarii / incydentów

    1. Wszyscy pracownicy mają obowiązek zgłaszania do Administratora wszelkich zdarzeń, które naruszają lub mogą naruszyć zasady bezpieczeństwa informacji.
    2. Błędy / awarie oraz pozostałe sprawy związane z infrastrukturą informatyczną należy zgłaszać do Administratora Systemów Informatycznych.

4. Postanowienia końcowe

    1. Niniejsza Instrukcja jest dokumentem wewnętrznym i nie może być udostępniania osobom nieupoważnionym w żadnej formie.
    2. Wszyscy upoważnieni zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Instrukcji.
    3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z Instrukcji stanowić mogą podstawę do pociągnięcia danej osoby do odpowiedzialności, adekwatnie do łączącego ją z Administratorem stosunku prawnego
    4. W sprawach nieuregulowanych w niniejszej Instrukcji mają zastosowanie przepisy Ustawy oraz wydanych na jej podstawie aktów wykonawczych.

Historia zmian

Data	Zakres zmian	Opracował	Sprawdził	Zatwierdził
	Wydanie pierwsze	Anna Martyna		