Załącznik do zarządzenia Nr 130/2009
Kierownika Ośrodka Pomocy Społecznej
Gminy Lubawa z dnia 30 grudnia 2009r.

Instrukcja Zarządzania Systemami Informatycznymi w Ośrodku Pomocy Społecznej Gminy Lubawa

Opracowali :

Administrator Bezpieczeństwa Informacji
Referent Ośrodka Pomocy Społecznej Gminy Lubawa
Marcin Kulkowski

Zastępca Administratora Bezpieczeństwa Informacji
Referent Ośrodka Pomocy Społecznej Gminy Lubawa
Lucyna Gacioch

ROZDZIAŁ 1
Podstawa prawna

§ 1

§ 3 i 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i Systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

Postanowienia ogólne

§ 2

Instrukcja Zarządzania Systemami Informatycznymi jest dokumentem eksploatacyjnym, regulującym zasady oraz procedury zarządzania i administrowania Systemami Informatycznymi w Ośrodku Pomocy Społecznej Gminy Lubawa. Instrukcja obejmuje swoim zakresem wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemach informatycznych.

§ 3

Określenia i skróty użyte w Instrukcji oznaczają:

1. Administrator danych osobowych – Kierownik Ośrodka Pomocy Społecznej Gminy Lubawa, zwany dalej Kierownikiem.
2. ABI - Administrator Bezpieczeństwa Informacji – osoba wyznaczona przez Administratora danych osobowych tj. informatyk, do nadzorowania przestrzegania zasad ochrony danych osobowych. Ponadto osoba odpowiedzialna za wdrożenie i stosowanie zasad bezpieczeństwa systemów informatycznych, zobowiązana do stosowania technicznych i organizacyjnych środków ochrony przewidzianych w systemach informatycznych.
3. Użytkownik systemu – osoba posiadająca upoważnienie do wprowadzania i przetwarzania danych w systemie informatycznym w zakresie wskazanym w upoważnieniu.
4. Ustawa – ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.),
5. Hasło – ciąg znaków literowych, cyfrowych lub innych specjalnych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
6. Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych specjalnych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w systemie informatycznym.
7. Sieć LAN/WAN – sieć lokalna/rozległa umożliwiająca połączenie systemów informatycznych przy wykorzystaniu specjalistycznych dedykowanych urządzeń i sieci telekomunikacyjnych.
8. Dane sensytywne – 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 informacje o innych orzeczeniach wydanych w postępowaniu sądowym lub administracyjnym.
9. Rejestr udostępnionych danych osobowych – rejestr, w którym odnotowywane są informacje o odbiorcach danych z systemu/aplikacji, prowadzony dla danego systemu/aplikacji.

ROZDZIAŁ 2
Procedury nadawania, zmiany uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemach informatycznych

§ 4

1. Każdy użytkownik przed przystąpieniem do przetwarzania danych zapoznaje się z:
   - Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Ośrodku Pomocy Społecznej Gminy Lubawa,
   - niniejszą instrukcją

   oraz otrzymuje upoważnienie do przetwarzania danych osobowych wydane przez Administratora danych osobowych.
2. Opis procedury nadawania/odbierania uprawnień dostępu do lokalnej sieci komputerowej przedstawiony jest poniżej. Stosowany w Ośrodku schemat uprawnień dostępu do sieci LAN/WAN zakłada, iż użytkownicy uzyskują dostęp do sieci na z góry zdefiniowanym poziomie użytkownika w zależności od zakresu obowiązków i powierzonych zadań do wykonania na danym stanowisku.
3. ABI rejestruje/usuwa użytkownika w systemie i nadaje mu wymagane uprawnienia.
4. ABI informuje użytkownika o fakcie nadania/odebrania uprawnień. W przypadku nadania uprawnień, informuje dodatkowo o założonym koncie i nadanych uprawnieniach.
5. Użytkownik po otrzymaniu od ABI informacji o założonym koncie z wymaganymi uprawnieniami, wykonuje:
   a) loguje się do systemu/aplikacji w celu sprawdzenia poprawności konta i uprawnień,
   b) przy pierwszym logowaniu się do systemu/aplikacji użytkownik musi zmienić nadane mu przez ABI hasło.
6. Użytkownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.

§ 5

1. Powyższe zasady nadawania/odbierania uprawnień dostępu do wszystkich systemów/aplikacji eksploatowanych w Ośrodku obowiązują wszystkich pracowników.
2. W przypadku gdy system/aplikacja nie posiada wbudowanych mechanizmów kontroli dostępu, wówczas należy niezwłocznie rozbudować taki system/aplikacje o te mechanizmy, a do czasu wdrożenia takich mechanizmów należy zaimplementować ograniczenia dostępu na poziomie systemu operacyjnego, bądź ograniczenia proceduralne.

ROZDZIAŁ 3
Metody i środki uwierzytelniania w systemach informatycznych

§ 6

1. Naczelna zasadą bezpieczeństwa systemów/aplikacji i sieci IT jest ochrona informacji przed nieuprawnionym dostępem, ujawnieniem, przypadkowym lub nieautoryzowanym zniszczeniem lub modyfikacją danych. Stosowanie zasad uwierzytelniania użytkowników systemów/aplikacji (a tym sieci LAN/WAN) ma bezpośredni wpływ na zachowanie poufności, rozliczalności oraz integralności danych.

§ 7

1. W systemach/aplikacjach informatycznych Ośrodka stosuje się dwustopniowe uwierzytelnianie na poziomie:
    a) dostępu do sieci LAN/WAN,
    b) dostępu do systemu/aplikacji.
2. Do uwierzytelniania użytkownika w systemie/aplikacji na obu poziomach używa się identyfikatorów lub haseł:
    a) stosowanie unikalnych identyfikatorów użytkownika zapewnia bezpieczeństwo i realizuje zasady rozliczalności w systemach i sieciach teleinformatycznych Ośrodka,
    b) zasada ta ma na celu przypisanie w sposób jednoznaczny wszelkich działań w systemie konkretnemu użytkownikowi (nie dopuszcza się aby użytkownik korzystał z kont: administrator, gość, a także z konta innego użytkownika),
    c) ograniczenie dostępu do informacji jedynie do kręgu użytkowników uprawnionych (autoryzowanych) wymaga przyjęcia odpowiednio dobrej polityki stosowania haseł.
3. W Ośrodku stosuje się poziom bezpieczeństwa przetwarzania danych adekwatnie do klasyfikacji tych danych w systemach/aplikacjach. W związku z powyższym obowiązujące są trzy poziomy bezpieczeństwa:
    a) poziom podstawowy – dla systemów/aplikacji, w których nie są przetwarzane dane osobowe sensytywne oraz żadne urządzenie systemu informatycznego służące do przetwarzania danych osobowych nie jest połączone z siecią publiczną. Wówczas hasło na poziomie dostępu do systemu/aplikacji musi składać się z co najmniej 6-ciu znaków,
    b) poziom podwyższony – dla systemów/aplikacji, w których są przetwarzane dane sensytywne oraz żadne urządzenie systemu informatycznego służące do przetwarzania danych osobowych nie jest połączone z siecią publiczną. Wówczas hasło na poziomie dostępu do systemu/aplikacji musi składać się z co najmniej 8-ciu znaków i musi zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,
    c) poziom wysoki - dla systemów/aplikacji, w których są przetwarzane dane sensytywne oraz co najmniej jedno urządzenie systemu informatycznego służące do przetwarzania danych osobowych nie jest połączone z siecią publiczną. Wówczas stosowane są środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelniania.
4. Hasło dostępu do sieci LAN/WAN musi składać się z minimum 6 znaków, w tym jeden znak specjalny i cyfra.
5. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów bądź innych bezpośrednio kojarzących się z użytkownikiem.
6. Hasło nie może być ujawnione innej osobie nawet po utracie ważności hasła.
7. System automatycznie powinien wymuszać zmianę hasła nie rzadziej niż jeden raz w miesiącu. Hasło musi być zmienione przez użytkownika.

§ 8

1. Procedura zarządzania środkami uwierzytelniania:
    a) ABI nadaje hasło dostępu do systemu/aplikacji lub sieci LAN/WAN dla nowego użytkownika albo użytkownika, który zapomniał swojego ostatniego hasła,
    b) użytkownik systemu/aplikacji niezwłocznie ustala swoje, znane tylko jemu hasło, po nadaniu hasła przez ABI. System automatycznie wymusza na użytkowniku zmianę nadanego przez administratora hasła przy pierwszym

logowaniu,
c) użytkownik systemu nie może w dowolnym momencie zmienić swojego hasła dostępu do systemu/aplikacji, tylko ABI ma do tego uprawnienia i na prośbę użytkownika może to zrobić,
d) obowiązuje bezwzględny zakaz notowania w jakiejkolwiek formie obecnych oraz wygasłych haseł dostępu.

ROZDZIAŁ 4
Rozpoczęcie, zawieszenie i zakończenie pracy przez użytkowników systemów

§ 9

1. Procedura rozpoczęcia pracy:
   a) uruchomić komputer wchodzący w skład systemu informatycznego, podłączony fizycznie do sieci lokalnej i zalogować się podając własny identyfikator i hasło dostępu,
   b) jeśli użytkownik wprowadzi 5-krotnie błędnie hasło wówczas jego identyfikator i hasło zastaną zablokowane. W celu odblokowania swojego identyfikatora, użytkownik postępuje według procedury obowiązującej przy nadawaniu/odbieraniu uprawnień dostępu do systemów informatycznych opisanej w Rozdziale 2 § 4,
   c) uruchomić wybrany system/aplikację (w szczególności aplikację bazodanową m. in. przetwarzającą dane),
   d) zalogować się do systemu/aplikacji w sposób analogiczny do przedstawionego powyżej.
2. Procedura zawieszenia pracy w systemie/aplikacji. Przy każdorazowym opuszczeniu stanowiska komputerowego, należy dopilnować, aby na ekranie nie były wyświetlane informacje lub dane, poprzez zablokowanie komputera. Każdy użytkownik ma obowiązek stosowania wygaszacza ekranu zabezpieczonego hasłem lub wyłączeniem monitora lub wylogowania się z systemu.
3. Procedura zakończenia pracy w systemie:
   a) zamknąć system/aplikację,
   b) zamknąć system operacyjny komputera i zaczekać na jego wyłączenie,
   c) wyłączyć monitor,
   d) sprawdzić czy elektroniczne nośniki informacji zawierające dane osobowe nie zostały pozostawione bez nadzoru.
4. Użytkownik w pełnym zakresie odpowiada za powierzony mu sprzęt komputerowy i wykonane czynności aż do momentu rozliczenia ze sprzętu komputerowego.

ROZDZIAŁ 5
Procedury tworzenia kopii zapasowych danych

§ 10

1. W celu zapewnienia optymalnego poziomu ochrony danych gromadzonych w systemach informatycznych Ośrodka, przyjęto do stosowania zasadę przetwarzania informacji zawartych w bazach Ośrodka w oparciu o architekturę klient-serwer. Wynika stąd praktyka przetwarzania danych w bazach na dedykowanych dla systemu/aplikacji serwerach.
2. Jeśli stosowane dotychczas rozwiązania nie są zgodne z architekturą klient-serwer, to należy zapewnić możliwość przechowywania gromadzonych za ich pomocą danych na wyznaczonym serwerze plików.
3. Indywidualne stanowiska komputerowe, do których dostęp posiadają pracownicy

Ośrodka, stanowią jedynie końcówki klienckie systemu komputerowego.
4. Wszelkie informacje (w tym dane osobowe) przetwarzane przy pomocy uruchamianych na poszczególnych stanowiskach aplikacjach bazodanowych są zapisywane bezpośrednio na serwerach.
5. Opisywana tu zasada przetwarzania danych wpływa bezpośrednio na zagadnienia związane z tworzeniem kopii bezpieczeństwa systemów.

§ 11

1. Kopie zapasowe baz danych oraz aplikacji bazodanowych zlokalizowanych na serwerach wykonane są:
    a) w cyklu dobowym (w godzinach nocnych) za pomocą aplikacji archiwizujących dane do postaci kopii pełnych (zawierających zapis jedynie tych informacji, które podczas ostatniej doby uległy zmianie),
    b) w cyklu miesięcznym tworzony jest „ręczny”, pełny backup systemu (łącznie z kopią systemu operacyjnego serwera),
    c) dodatkowo kopie wykonywane są każdorazowo przed wykonaniem aktualizacji w systemach bazodanowych.
2. ABI sprawuje nadzór nad wykonywaniem w/w kopii zapasowych oraz weryfikuje ich poprawność.
3. Zasady przechowywania kopii:
    a) kopie zapasowe zapisywane są na nośnikach CD, DVD i macierzy dyskowej,
    b) kopie zapasowe zbioru danych oraz oprogramowania i narzędzi programistycznych zastosowanych do przetwarzania danych są przechowywane w przeznaczonej do tego celu metalowej szafie, znajdującej się w wyznaczonym pomieszczeniu w Budynku E Urzędu Gminy Lubawa w Biurze IT,
    c) dostęp do metalowej szafy mają tylko upoważnienie pracownicy, tj. ABI oraz osoba zastępująca ABI podczas jego nieobecności,
    d) czas przechowywania kopii zapasowych określony został w dokumentacji przetwarzania i ochrony danych osobowych w Rozdziale 6 Instrukcji).

ROZDZIAŁ 6
Przechowywanie elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

§ 12

1. Elektroniczne nośniki informacji:
    a) dane w postaci elektronicznej przetwarzane w systemie zapisane na nośnikach materialnych (np. dyskietkach, dyskach magnetooptycznych, taśmach magnetycznych, pendrive-ach czy dyskach twardych) są własnością Ośrodka,
    b) w/w elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych,
    c) po zakończeniu pracy przez użytkownika systemu/aplikacji, w/w elektroniczne nośniki informacji są przechowywane w meblach biurowych,
    d) elektroniczne nośniki informacji, o których mowa powyżej powinny być oznaczone w sposób umożliwiający ich identyfikację.
2. Przekazywanie i niszczenie elektronicznych nośników informacji:
    a) elektroniczne nośniki informacji zawierające dane osobowe można przekazywać tylko podmiotom lub osobom uprawnionym na podstawie przepisów prawa, za zgodą osoby do tego upoważnionej przez Administratora Danych Osobowych,
    b) dane osobowe na każdym nośniku zewnętrznym powinny być zabezpieczone

przed odczytem (minimum hasłem),
c) dane osobowe przenoszone za pomocą zewnętrznych nośników informacji powinny być z nich trwale usunięte po poprawnym ich przeniesieniu na docelowy sprzęt komputerowy i do docelowej bazy danych,
d) przekazanie i niszczenie elektronicznych nośników informacji zawierających dane osobowe, odbywa się na podstawie protokołu podpisanego przez ABI oraz właściwych użytkowników.

ROZDZIAŁ 7
Środki ochrony systemów informatycznych

§ 13

1. Poniżej przedstawiono zasady ochrony systemów przetwarzania danych przed tzw. „szkodliwym oprogramowaniem" oraz próbami penetracji przez osobowy nieuprawnione.
2. Ochrona antywirusowa:
   a) za ochronę antywirusową odpowiada ABI,
   b) czynności związane z ochroną antywirusową systemu informatycznego wykonuje ABI wykorzystując w trakcie pracy systemu informatycznego moduły programu antywirusowego w aktualnej wersji, sprawdzającego na bieżąco zasoby systemu informatycznego,
   c) oprogramowanie antywirusowe jest instalowane centralnie na serwerze oraz na wszystkich stanowiskach komputerowych podłączonych do sieci,
   d) aktualizacja oprogramowania antywirusowego odbywa się nie rzadziej niż raz w tygodniu w sposób automatyczny dla wszystkich komputerów zainstalowanych w sieci,
   e) instalacja oprogramowania antywirusowego oraz jego aktualizacja na komputerach niepodłączonych do sieci, odbywa się rzadziej niż raz w tygodniu i jest wykonywana przy zastosowaniu nośników zewnętrznych przez ABI,
   f) użytkownik systemu na stanowisku komputerowym, importujący dane do systemu informatycznego, jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości występowania wirusów i szkodliwego oprogramowania,
   g) w przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe na którym wykryto wirusa oraz wszystkie posiadane przez użytkownika nośniki,
   h) kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.

§ 14

1. ABI jest odpowiedzialny za aktywowanie i poprawną konfigurację specjalistycznego oprogramowania monitorującego wymianę danych na styku:
   a) sieci lokalnej i sieci rozległej (LAN/WAN),
   b) stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.
2. ABI obowiązany jest do utrzymywania stałej aktywności zainstalowanego specjalistycznego oprogramowania monitorującego wymianę danych oraz do jego aktualizacji.
3. Ochrona przed awarią zasilania:
   a) system, w którym przetwarzane są dane osobowe powinien posiadać mechanizmy pozwalające zabezpieczyć je przed ich utratą lub

nieautoryzowaną zmianą spowodowaną awaria zasilania lub zakłóceniami w sieci zasilającej,
b) dane osobowe przetwarzane w systemie chroni się stosując filtry zabezpieczające przed skutkami spadku napięcia oraz urządzenia podtrzymujące zasilanie do momentu poprawnego zapisania danych i wylogowania się użytkownika z systemu,
c) dane osobowe przetwarzane z wykorzystaniem serwera w wewnętrznych sieciach teleinformatycznych należy zabezpieczyć przed zanikiem napięcia wykorzystując centralny UPS i generator prądu.

ROZDZIAŁ 8
Monitorowanie dostępu do danych

§ 15

1. Dla każdego systemu, w którym przetwarzane są dane osobowe, prowadzony jest Rejestr, w którym odnotowywane są informacje o odbiorcach danych z tego systemu (o ile występuje dla danego systemu proces udostępniania danych osobom wymienionym w § 15 ust. 2).
2. Odbiorcą danych jest każdy, komu udostępnia się dane:
   a) osoby, której dane dotyczą,
   b) podmiotu, któremu powierzono przetwarzanie danych,
   c) organów państwowych luba organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
3. Odnotowanie obejmuje informacje o:
   a) nazwie jednostki organizacyjnej lub imieniu i nazwisku osobowy, której udostępniono dane,
   b) zakresie udostępnianych danych,
   c) dacie udostępnienia.
4. Obowiązek odnotowania w/w informacji w Rejestrze spoczywa na użytkowniku systemu udostępniającemu dane.
5. Odnotowanie informacji w Rejestrze powinno nastąpić niezwłocznie po udostępnieniu danych.
6. Na podstawie art. 29 ustawy o ochronie danych osobowych (Dz. U. z 2002r. Nr 101 poz. 929, z późn. zm.) udostępnianie danych osobowych może nastąpić w następujących przypadkach:
   a) w celu innym niż włączenie danych do zbioru – Administrator udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa,
   b) dane osobowe, z wyłączeniem danych sensytywnych mogą być także udostępnione w celach innych niż włączenie do zbioru, innym osobom i podmiotom niż wymienione w § 15 ust. 6 lit. a), jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą,
   c) dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.
7. Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
8. Na żądanie osoby, której dane zostały udostępnione, informacje o udostępnionych danych są zamieszczane w raporcie z Rejestru, a raport przekazywany tej osobie.
9. Nadzór nad prawidłowością odnotowywania w Rejestrze w/w informacji sprawuje ABI.

ROZDZIAŁ 9
Procedury wykonywania przeglądów i konserwacji systemu

§ 16

1. Dla zachowania ciągłości pracy i bezpieczeństwa danych przeprowadza się przegląd i konserwację platformy sprzętowej, na której eksploatowany jest system/aplikacja.
2. Przeglądy i konserwacja urządzeń:
    a) przeglądy i konserwacja urządzeń wchodzących w skład platformy sprzętowej dla systemu/aplikacji powinny być wykonywane w terminach określonych przez producenta sprzętu,
    b) jeśli producent nie przewidział dla danego urządzenia potrzeby dokonywania przeglądów eksploatacyjnych lub też nie określił ich częstotliwości, to o dokonaniu przeglądu oraz sposobie jego przeprowadzenia decyduje ABI,
    c) przegląd i konserwacja urządzeń może być wykonana na żądanie przełożonego ABI,
    d) czynności, o których mowa w § 16 ust. 2 lit. a i lit. b wykonuje ABI co najmniej jeden raz na kwartał,
    e) nieprawidłowości ujawnione w trakcie przeglądów bądź konserwacji, powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane przez ABI,
    f) za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ABI.

§ 17

1. Przegląd systemów/aplikacji i narzędzi programistycznych przeprowadzany jest w celu sprawdzenia poprawności działania i wykonywany jest w następujących przypadkach:
    a) zmiany wersji oprogramowania systemu/aplikacji,
    b) zmiany wersji oprogramowania na stanowisku komputerowym użytkownika,
    c) zmiany systemu operacyjnego platformy sprzętowej, na której eksploatowany jest system/aplikacja,
    d) zmiany systemu operacyjnego na stanowisku komputerowym użytkownika,
    e) wykonania zmian w systemie/aplikacji spowodowanych koniecznością naprawy lub modyfikacji systemu.
2. Przed dokonaniem zmian w systemie/aplikacji należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych, na testowej bazie danych. Sprawdzenie powinno m.in. obejmować:
    a) poprawność logowania się do systemu w zależności od posiadanych uprawnień (zasymulować pracę wszystkich typów uprawnień użytkownika),
    b) poprawność działania funkcjonalności systemu/aplikacji sprawdzonej na różnego typu danych,
    c) poprawność działania wszystkich elementów aplikacji (menu, zestawienia, formularze, raport, itp.).
3. Za prawidłowość przeprowadzenia procesu przeglądu i konserwacji systemu/aplikacji odpowiada ABI.

§ 18

Konserwacja systemów/aplikacji wykorzystywanych przez użytkowników.

1. Konserwację oprogramowania przeprowadza się po zgłoszeniu przez użytkownika systemu/aplikacji potrzeby wprowadzenia zmian pozwalających dostosować funkcjonalność systemu/aplikacji do obsługi bieżących i planowanych potrzeb Ośrodka. Zgłoszenie kierowane jest do ABI.
2. Przed wdrożeniem wymaganych przez użytkownika zmian w systemie/aplikacji

informatycznej, należy dokonać sprawdzenia poprawności działania zmodyfikowanego systemu/aplikacji w warunkach testowych na testowej bazie danych na takich samych zasadach jak ma to miejsce w przypadku przeglądu oprogramowania, opisanych w § 17 ust. 3.

3. Konserwację systemu/aplikacji przeprowadza się w obecności użytkownika.

ROZDZIAŁ 10
Postanowienia końcowe

§ 19

W sprawach nie uregulowanych niniejszą Instrukcją zastosowanie znajdują:

1. Norma PN-I-13335-1 „Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych”.
2. Norma PN-ISO/IEC-17799 „Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji.
3. Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.).
4. Rozporządzenie Ministra Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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. Nr 100, poz. 1024).