Załącznik nr 3

ZATWIERDZAM

DYREKTOR
Zespołu Wojewódzkich Przychodni Specjalistycznych
w Katowicach
Grzegorz Nowaczyński

Instrukcja Zarządzania Systemem Informatycznym

ZWPS

Spis treści

Załączniki do Instrukcji:

A. Regulamin korzystania z Sieci LAN/WAN oraz systemów bądź aplikacji.
B. Zasady użytkowania sprzętu komputerowego przez pracowników ZWPS
C. Zasady udzielania pomocy użytkownikom sprzętu komputerowego w ZWPS.

Rozdział 1

Postanowienia ogólne.

§ 1

Instrukcja Zarządzania Systemami Informatycznymi jest dokumentem eksploatacyjnym, regulującym zasady oraz procedury zarządzania i administrowania Systemami Informatycznymi ZWPS w Katowicach. Instrukcja obejmuje swoim zakresem wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemach informatycznych, w szczególności zaś osoby pełniące funkcje:

1. Administratora Bezpieczeństwa Informacji;
2. Administratorów Systemów Informatycznych;
3. bezpośrednich przełożonych osób przetwarzających dane osobowe;
4. inne osoby wskazane przez Administratora Danych Osobowych, w tym osoby z podmiotów zewnętrznych współpracujące z ZWPS i współuczestniczące w procesie przetwarzania danych osobowych.

§ 2

Określenia i skróty użyte w Instrukcji oznaczają:

1. Administratorze Danych – rozumie się przez to administratora danych – ZWPS w Katowicach reprezentowanego przez Dyrektora, decydującego o celach i środkach przetwarzania danych osobowych,,
2. Administratorze Bezpieczeństwa Informacji – rozumie się przez to osobę, której administrator danych powierzył pełnienie obowiązków administratora bezpieczeństwa informacji zwany dalej „ABI".
3. Administratorze Systemu Informacji – rozumie się przez to osobę, której administrator danych powierzył pełnienie obowiązków administratora systemu informacji.
4. Danych osobowych - uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
5. Przełożony użytkownika, zwany dalej przełożonym – osoba odpowiedzialna za przestrzeganie zasad przetwarzania i ochrony danych przez podległych mu pracowników.
6. Osobie możliwej 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, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

7. 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 funkcjonalnie.
8. Haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi.
9. Identyfikatorze – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
10. Integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
11. Odbiorcy danych – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
    - osoby, której dane dotyczą,
    - osoby upoważnionej do przetwarzania danych,
    - przedstawiciela, o którym mowa w art. 31a ustawy,
    - podmiotu, o którym mowa w art. 31 ustawy,
    - organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
12. Osobie upoważnionej do przetwarzania danych osobowych – rozumie się przez to osobę, która upoważniona została do przetwarzania danych osobowych przez Dyrektora ZWPS na piśmie,
13. Poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
14. Przetwarzającym – rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawieranej zgodnie z art. 31 ustawy,

15. Raporcie – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,

16. Rozliczalność – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

17. Rozporządzeniu – rozumie się przez to 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 (Dz. U nr 100, poz. 1024),

18. Publicznej sieci telekomunikacyjnej – rozumie się przez to publiczną sieć telekomunikacyjną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U nr 171, poz. 1800 z póź. zm.),

19. Sieci telekomunikacyjnej – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U nr 171, poz. 1800 z póź. zm.),

20. Serwisancie – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego,

21. Systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

22. Teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,

23. Ustawie – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U z 2002 r. nr 101, poz. 926 z póź. zm.),

24. Uwierzytelnianiu – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

25. Użytkowniku – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło.

26. przetwarzaniu 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,

27. zabezpieczeniu danych w systemie informatycznym – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,

28. usuwaniu danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,

29. zgodzie osoby, której dane dotyczą – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści,

30. szyfrowaniu – rozumie się przez to zabezpieczenie danych poprzez uczynienie ich nieczytelnymi bez znajomości właściwego klucza/hasła i programu zawierającego algorytm kryptograficzny pozwalający na odczyt danych tylko osobom znającym klucz/hasło.

31. Sieć LAN/WAN – sieć lokalna/rozległa umożliwiająca połączenie systemów informatycznych przy wykorzystaniu specjalistycznych dedykowanych urządzeń i sieci telekomunikacyjnych w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.).

Pozostałe definicje wynikają z ustawy.

Rozdział 2

Procedury nadawania, zmiany uprawnień do przetwarzania danych i rejestrowania uprawnień w systemach informatycznych.

§ 3

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych zapoznaje się z:
   a) niniejszą instrukcją oraz:
      - Załącznik A. Regulamin korzystania z Sieci LAN/WAN oraz systemów bądź aplikacji przez pracowników,
      - Załącznik B. Zasady użytkowania sprzętu komputerowego przez pracowników w ZWPS,
      - Załącznik C. Zasady udzielania pomocy użytkownikom sprzętu komputerowego w ZWPS,

   b) procedurami określonymi przez Administratora Danych Osobowych.

2. Podstawą nadania uprawnień do przetwarzania danych w systemie informatycznym jest wniosek przełożonego i podpisane przez ABI upoważnienie do przetwarzania danych osobowych.

§ 4

1. Opis procedury nadawania/odbierania uprawnień dostępu do lokalnej sieci komputerowej przedstawiony jest poniżej. Stosowany w ZWPS 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.
2. Kierownik Działu Kadr:
   a) wnioskuje do ABI o nadanie/odebranie pracownikowi uprawnień do przetwarzania danych w systemach/aplikacjach eksploatowanych w sieci LAN/WAN w związku z wykonywanymi przez niego zadaniami,
3. ABI na podstawie wniosku, wykonuje lub zleca ASI:
   a) rejestruje/usuwa użytkownika w systemie i nadaje mu wymagane uprawnienia,
   b) informuje przełożonego użytkownika o fakcie nadania/odebrania uprawnień. W przypadku nadania uprawnień, informuje dodatkowo o założonym koncie wnioskowanym dla użytkownika i nadanych uprawnieniach,
   c) w przypadku, gdy nadanie pracownikowi wymaganych uprawnień może grozić naruszeniem standardów bezpieczeństwa systemów/aplikacji pracujących w sieci, ABI informuje przełożonego użytkownika o tym zagrożeniu i wstrzymuje proces nadawania uprawnień.
4. Użytkownik, po otrzymaniu od ASI 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.
5. Powyższy schemat nadania/odebrania uprawnień dostępu do systemów/aplikacji eksploatowanych w sieci LAN/WAN należy stosować również w przypadku wymaganej zmiany w istniejących uprawnieniach użytkownika.

§ 5

1. Powyższe zasady nadawania/odbierania uprawnień dostępu do wszystkich systemów/aplikacji eksploatowanych w ZWPS 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. Naczelną 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 (w tym sieci LAN/WAN) ma bezpośredni wpływ na zachowanie poufności, rozliczalności oraz integralności danych.

§ 7

1. W systemach/aplikacjach informatycznych ZWPS stosuje się uwierzytelnienie dwustopniowe, na poziomie:
   a) dostępu do systemu,
   b) dostępu do aplikacji.
2. Do uwierzytelnienia użytkownika w systemie/aplikacji na obu poziomach używa się identyfikatorów, haseł lub karty inteligentnej.
   a) stosowanie unikalnych identyfikatorów użytkownika zapewnia bezpieczeństwo i realizuje zasady rozliczalności w systemach i sieciach teleinformatycznych,
   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 dobranej polityki stosowania haseł.

3. W ZWPS, 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 się składać 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 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 jest połączone z siecią publiczną. Wówczas Administrator danych musi dodatkowo stosować środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelniania.

4. 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.

5. Hasło nie może być ujawnione innej osobie nawet po utracie ważności hasła.

6. System automatycznie powinien wymuszać zmianę hasła nie rzadziej, niż jeden raz w miesiącu. Hasło musi być zmienione przez użytkownika niezwłocznie w przypadku podejrzenia lub stwierdzenia jego ujawnienia.

§ 8

1. Procedura zarządzania środkami uwierzytelniania

   a) ASI na wniosek ABI nadaje hasło dostępu do systemu/aplikacji dla nowego użytkownika albo dla użytkownika, który zapomniał swojego ostatniego hasła,

   b) użytkownik systemu/aplikacji niezwłocznie ustala swoje, znane tylko jemu hasło, po nadaniu hasła przez ASI. System automatycznie wymusza na użytkowniku zmianę nadanego przez administratora hasła przy pierwszym logowaniu,

c) użytkownik systemu w dowolnym momencie może zmienić swoje hasło dostępu do systemu/aplikacji,

d) obowiązuje bezwzględny zakaz notowania w jakiejkolwiek formie obecnych oraz wygasłych haseł dostępu,

ASI zapisuje swój identyfikator oraz hasła dostępu po każdej ich zmianie i umieszcza je w kopercie, a następnie przekazuje zamkniętą kopertę do przechowania w wyznaczonej do tego celu szafie pancernej ulokowanej w Sekretariacie. Koperta taka może być awaryjnie udostępniona innemu administratorowi za zgodą ABI. ABI odpowiedzialny jest za prowadzenie rejestru udostępnionych awaryjnie haseł. Po awaryjnym użyciu hasła, musi ono zostać jak najszybciej zmienione przez właściwego ABI.

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 3-krotnie błędnie hasło, wówczas jego identyfikator i hasło zostaną zablokowane. W celu odblokowania swojego identyfikatora, użytkownik zgłasza się do ASI celem odblokowania użytkownika,

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 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 wykonywane 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 ZWPS, przyjęto do stosowania zasadę przetwarzania informacji zawartych w bazach danych w oparciu o architekturę klient – serwer. Wynika stąd praktyka przetwarzania danych w bazach danych 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 ZWPS, 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. W szczególnych przypadkach, za zgodą ABI, aplikacje oraz dane, w tym dane osobowe, mogą być przechowywane lokalnie na stanowiskach komputerowych niepodłączonych do sieci LAN/WAN. W takich przypadkach obowiązek wykonania kopii bezpieczeństwa aplikacji oraz codziennego wykonywania kopii bezpieczeństwa bazy danych oraz ich bezpiecznego przechowywania (zgodnie z zasadami opisanymi w poniższym § 11 ust.3), spoczywa bezpośrednio na użytkowniku danej aplikacji.

6. 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 wykonywane są:
   a) w cyklu dobowym (w godzinach nocnych) za pomocą aplikacji archiwizujących dane do postaci tzw. kopii przyrostowych (zawierających zapis jedynie tych informacji, które podczas ostatniej doby uległy zmianie),
   b) w cyklu tygodniowym, podobnie przy użyciu oprogramowania aplikacji archiwizujących, tworzone są pełne kopie baz danych oraz aplikacji,
   c) w cyklu miesięcznym tworzony jest „ręczny", pełny backup systemu (łącznie z kopią systemu operacyjnego serwera).
2. ASI sprawuje nadzór nad wykonywaniem ww. kopii zapasowych oraz weryfikuje ich poprawność.
3. Zasady przechowywania kopii
   a. kopie zapasowe zbioru danych oraz oprogramowania zastosowanego do przetwarzania danych są przechowywane w osobnym pomieszczeniu zlokalizowanym w osobnym skrzydle budynku ZWPS – szafa sieciowa piętro I.
   b. dostęp do pomieszczenia z kopiami mają tylko upoważnieni pracownicy,
4. Plik z rejestrem kopi zapasowych znajduje się na serwerze przechowującym kopie zapasowe.

Rozdział 6

Przechowywanie nośników informacji zawierające dane oraz kopii zapasowych

§ 12

1. Elektroniczne nośniki informacji

1. dane w postaci elektronicznej przetwarzane w systemie zapisane na nośnikach materialnych (np. pamięciach FLASH, dyskach optycznych, dyskach twardych) są własnością ZWPS,

2. wyżej wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych,
3. po zakończeniu pracy przez użytkowników systemu/aplikacji, ww. elektroniczne nośniki informacji są przechowywane w meblach biurowych ze sprawnym zamknięciem lub w kasetkach,
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 ABI,
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 ASI oraz właściwych użytkowników. Protokół zatwierdzony przez przełożonego użytkownika należy przekazać ABI

Rozdział 7

Środki ochrony systemów informatycznych

§ 13

1. Poniżej przedstawiono zasady ochrony systemów przetwarzania danych przed tzw. „szkodliwym oprogramowaniem" oraz próbami penetracji przez osoby nieuprawnione.
2. Ochrona antywirusowa

a) za ochronę antywirusową odpowiada ASI,
b) czynności związane z ochroną antywirusową systemu informatycznego wykonuje ASI, 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 nie rzadziej niż raz w miesiącu i jest wykonywana przy zastosowaniu nośników zewnętrznych,

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.

§ 14

1. ASI 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. ASI 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 awarią 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 zabezpieczać przed zanikiem napięcia wykorzystując UPS

Rozdział 8

Procedury wykonywania przeglądów i konserwacji systemów.

§ 15

W wypadku wystąpienia takiej potrzeby, lecz nie rzadziej niż raz na rok, ABI wykonuje przegląd przestrzegania instrukcji zarządzania systemem informatycznym, dokonuje przeglądu i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych. Wykryte podczas przeglądu i konserwacji nieprawidłowości w działaniu sprzętu lub programów służących do przetwarzania danych osobowych, usuwa się niezwłocznie. Osoba dokonująca wyeliminowania opisanych nieprawidłowości, zawiadamia o podjętych czynnościach Administratora Danych. Przegląd i konserwacja mogą być zlecone podmiotowi zewnętrznemu specjalizującemu się w tego typu działaniach. W wypadku przekazania sprzętu lub nośników informacji służących do przetwarzania danych osobowych podmiotowi trzeciemu, pozbawia się je zapisanych danych osobowych w sposób, który uniemożliwi ich odtworzenie.

W obydwu przypadkach, zostaną zachowane szczególne warunki ostrożności, w celu zabezpieczenia danych osobowych przed dostępem osób nieuprawnionych.

Rozdział 9

Postanowienia końcowe.

§ 16

1. Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Instrukcji może być podstawą rozwiązania stosunku pracy bez wypowiedzenia z osobą, która dopuściła się naruszenia.
2. W sprawach nieuregulowanych w Instrukcji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (t.j. Dz.U. z 2002 r., Nr 101, poz. 926 z późn. zm.) oraz przepisy wykonawcze do tej Ustawy.
3. Użytkownicy systemu zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Instrukcji, w wypadku odrębnych od zawartych w niniejszej Instrukcji uregulowań występujących w innych procedurach obowiązujących w ZWPS użytkownicy systemu mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych przetwarzanych w systemie informatycznym

Załącznik A
Regulamin korzystania z Sieci LAN/WAN oraz systemów bądź aplikacji przez pracowników ZWPS

§ 1

1. Regulamin ustala zasady korzystania z sieci LAN/WAN ZWPS.
2. Dokumentem nadrzędnym w stosunku do niniejszego regulaminu jest Instrukcja Zarządzania Systemami Informatycznymi

§ 2

1. Sieć LAN/WAN tworzą:
    1. sieci lokalne poszczególnych jednostek organizacyjnych oraz łącza między nimi;
    2. serwery aplikacji usług sieciowych.

§ 3

1. Użytkownikiem sieci LAN/WAN jest każda osoba korzystająca z komputera podłączonego do sieci LAN/WAN.
2. Konto użytkownika sieci – login i hasło usługi Active Directory jednoznacznie identyfikujące użytkownika.
3. Konto pocztowe – adres postaci imie.nazwisko@zwps.pl wraz z loginem i hasłem.
4. Konta użytkownika sieci jest przydzielane pracownikom na podstawie wniosku przełożonego.
5. Pracownicy korzystają z poczty poprzez wskazanego przez ASI klienta pocztowego lub dowolną przeglądarkę internetową.
6. Pojemność skrzynek pocztowych pracowników może zostać ograniczona przez ASI z powodów technicznych. Po przekroczeniu limitu zostanie zablokowana możliwość otrzymywania wiadomości do momentu oczyszczenia skrzynki pocztowej. W uzasadnionych przypadkach na wniosek przełożonego użytkownika, ASI może zwiększyć wielkość skrzynki.
7. Pracownicy mają możliwość przechowywania swojej poczty na stacjach roboczych, wiąże się to jednak z tym, że pełna odpowiedzialność za ewentualną utratę danych jest po stronie użytkownika.
8. Dział Kadr niezwłocznie przekazuje dane dotyczące rozwiązania/zawarcia umowy o pracę z pracownikami Administratorowi Bezpieczeństwa Informacji.
9. W przypadku pracownika, z którym został rozwiązany stosunek pracy, ABI zleca ASI archiwizację danych tego użytkownika, a następnie blokadę konta

§ 4

1. Każdy użytkownik systemu powinien postępować zgodnie z powierzonymi mu obowiązkami, a w szczególności z poniższymi zasadami:

    1. używać poczty elektronicznej tylko do celów służbowych;
    2. korzystać z Internetu tylko do celów służbowych;
    3. korzystać z systemów/aplikacji ZWPS tylko do celów służbowych.

2. Zabronione jest:

    1. wysyłanie masowej, niezamówionej poczty, kierowanej do różnych odbiorców (spam);
    2. udostępnianie treści chronionych prawem autorskim (filmy lub utwory muzyczne);
    3. udostępnianie treści zakazanych (np. pornografia);
    4. nieuzasadnione wynoszenie danych zawartych na nośnikach poza ZWPS;
    5. instalowanie oprogramowania bez ważnych licencji.

3. Pracodawca zastrzega sobie prawo do monitorowania ruchu w sieci LAN/WAN, w zakresie określonym w powyższych ust. 1 i 2.
4. Jeżeli zaistnieje potrzeba podłączenia komputera prywatnego pracownika do sieci LAN/WAN, wymaga to następujących czynności:

    1. akceptacji przełożonego pracownika;
    2. powiadomienia ABI.

5. Zabrania się podejmowania prób wykorzystania obcego konta, uruchamiania aplikacji deszyfrujących hasła, prowadzenia działań mających na celu podsłuchiwanie lub przechwytywanie informacji przepływającej w sieci.
6. Zabrania się uruchamiania aplikacji, które mogą zakłócić i destabilizować pracę systemu lub sieci komputerowej, bądź naruszyć integralność zasobów systemowych.
7. W przypadku naruszenia zasad opisanych w ust. 1, 2, 4 i 5 ABI blokuje dostęp do konta użytkownika. O tym fakcie powiadamiany jest Administrator Danych i przełożony pracownika.
8. W przypadku stwierdzenia, że komputer dołączony do sieci LAN/WAN generuje strumień danych zakłócający pracę sieci lub wskazujący na używanie tego komputera jako niezarejestrowanego serwera danych, ABI ma prawo zablokować dostęp do/z tego komputera do czasu wyjaśnienia sprawy. O tym fakcie powiadamiany jest Administrator Danych i przełożony pracownika.

Załącznik B.

Zasady użytkowania sprzętu komputerowego przez pracowników ZWPS

1.

Zasady użytkowania sprzętu komputerowego przez pracowników ZWPS, zwane dalej zasadami, określają prawa i obowiązki użytkowników sprzętu komputerowego.

2.

Ilekroć w zasadach jest mowa o:

1. Pomoc Techniczna – rozumie się przez to informatyka przyjmującego i realizującego zgłoszone problemy dotyczące użytkowania sprzętu komputerowego i oprogramowania komputerowego;
2. sprzęcie komputerowym – rozumie się przez to komputer oraz urządzenia peryferyjne, w tym: monitor, drukarka, skaner, wymagające do swojego działania połączenia z komputerem;
3. nośniki informatyczne – urządzenia umożliwiające zapisywanie i przenoszenie danych (np. dyskietka, twardy dysk, płyta CD, pamięci masowe flash).

3.

Użytkownikowi systemu przysługuje prawo:

1. do korzystania ze sprzętu komputerowego i sieci LAN/WAN wyłącznie w zakresie powierzonych mu zadań;
2. do korzystania z oprogramowania komputerowego zgodnie z umowami i ustawą z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tj. Dz.U. z 2006 r., nr 90, poz. 631 z późn. zm.).

4.

Informacje zapisane na nośnikach informatycznych należą do pracodawcy.

5.

O przekazaniu sprzętu komputerowego użytkownikowi decyduje przełożony użytkownika.

6.

Użytkownik jest materialnie odpowiedzialny za sprzęt komputerowy, który otrzymał do wykonywania obowiązków służbowych.

7.

Informatycy prowadzą sprawy w zakresie użytkowania sprzętu komputerowego i oprogramowania komputerowego, a w szczególności:

1. współpracują z działem administracj nad wykonaniem umów, dotyczących zakupu/serwisu sprzętu i oprogramowania;
2. zabezpieczają sprawne działanie sprzętu komputerowego i oprogramowania;
3. zapewniają standardy sprzętu komputerowego i oprogramowania spełniające wymagania ZWPS.

8.

Każdy użytkownik posiada identyfikator i hasło lub kartę inteligentną, które zabezpieczają dostęp do komputera, sieci LAN/WAN, baz danych i skrzynki pocztowej użytkownika.

9.

Zabronione jest:

1. podłączanie przez użytkownika własnych urządzeń do sprzętu komputerowego lub sieci LAN/WAN;
2. podłączania innych urządzeń niż sprzęt komputerowy do wydzielonej sieci energetycznej do zasilania komputerów;
3. samodzielne instalowanie oprogramowania na komputerze;
4. przemieszczenia sprzętu komputerowego do innej lokalizacji (pokoju) lub zmiany użytkownika bez uzgodnienia z Pomocy Technicznej;
5. fizyczne ingerowanie w konfigurację sprzętową urządzeń;
6. udostępnianie swojego identyfikatora i hasła do pracy innym osobom;
7. pozyskiwanie informacji z komputerów innych użytkowników bez ich wiedzy;
8. wykonywanie czynności, które mogą spowodować zakłócenia lub awarię sieci LAN/WAN;
9. wynoszenie poza miejsce pracy nośników zawierających dane oraz przesyłanie danych pocztą elektroniczną na zewnątrz

10.

Na stanowiskach pracy, na których używany jest sprzęt komputerowy obowiązują szczegółowe zasady jego użytkowania:

1. zakaz spożywania posiłków przy sprzęcie komputerowym;
2. zapewnienie warunków umożliwiających swobodne działanie układu chłodzenia użytkowanego sprzętu komputerowego;
3. utrzymanie czystości przy stanowiskach komputerowych;
4. zapewnienie odpowiedniego miejsca na lokalizację sprzętu komputerowego;
5. ustawienie z dala od źródeł wilgoci, grzejników lub innych substancji mogących zakłócić prawidłowe działanie sprzętu komputerowego.

11.

Użytkownik sprzętu komputerowego przenośnego zobowiązany jest do zapoznania się i stosowania warunków umowy ubezpieczenia, jeżeli została zawarta.

Załącznik C.

Zasady udzielania pomocy użytkownikom sprzętu komputerowego

1.

Zasady udzielania pomocy użytkownikom sprzętu komputerowego w ZWPS, zwane dalej zasadami, określają zasady postępowania w przypadku wystąpienia problemów w użytkowaniu sprzętu komputerowego lub zainstalowanego oprogramowania

2.

Ilekroć w zasadach jest mowa o:

1. Pomoc Techniczna – rozumie się przez to informatyka przyjmującego i realizującego zgłoszone problemy dotyczące użytkowania sprzętu komputerowego i oprogramowania komputerowego;
2. sprzęcie komputerowym – rozumie się przez to komputer oraz urządzenia peryferyjne, w tym. monitor, drukarka, skaner, wymagające do swojego działania połączenia z komputerem.

3.

1. Zgłaszanie problemów z użytkowaniem sprzętu komputerowego i udzielanie pomocy użytkownikowi odbywa się w następujący sposób:

    1. użytkownik zgłasza awarię do Pomocy Technicznej, który odnotowuje zgłaszane problemy;
    2. Pomoc Techniczna rozwiązuje zgłoszony problem lub przekazuje zlecenie naprawy firmie zewnętrznej.

2. W miarę możliwości technicznych przedstawia użytkownikowi możliwości udostępnienia sprzętu zastępczego na czas naprawy.