Załącznik nr ...1.... do Zarządzenia Nr...27/2011.....
Domu Pomocy Społecznej dla Kombatantów w Biłgoraju
z dnia...06.września.2011 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

w

Domu Pomocy Społecznej dla Kombatantów w Biłgoraju

Spis treści

Rozdział I....3
POSTANOWIENIA OGÓLNE....3
Rozdział II....3
UPRAWNIENIA DO PRZETWARZANIA DANYCH....3
Rozdział III....3
ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM....3
Rozdział IV....4
PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZ UŻYTKOWNIKA SYSTEMU....4
Rozdział V....6
PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA....6
Rozdział VI....6
WYDRUKI, ELEKTRONICZNE NOŚNIKI INFORMACJI ZAWIERAJĄCE DANE OSOBOWE ORAZ KOPIE ZAPASOWE....6
Rozdział VII....7
ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO....7
Rozdział VIII....8
PRZEGLĄDY, KONSERWACJA SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH....8

Rozdział I

POSTANOWIENIA OGÓLNE

§1

1. Instrukcja zarządzania systemem informatycznym Domu Pomocy Społecznej dla Kombatantów w Biłgoraju, zwana dalej „instrukcją", jest wewnętrznym dokumentem Administratora Danych, skierowanym do osób zatrudnionych przy przetwarzaniu danych osobowych w systemie informatycznym.
2. Celem instrukcji jest ochrona systemu informatycznego. Określa ona sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych.
3. Instrukcja dotyczy wszystkich systemów informatycznych i programów komputerowych, za pomocą których można przetwarzać dane, zlokalizowanych w budynkach Domu Pomocy Społecznej dla Kombatantów.
4. Wszystkie osoby zatrudnione przy przetwarzaniu danych osobowych w systemach informatycznych są zobowiązane do postępowania zgodnie z zasadami określonymi w niniejszej instrukcji.
5. Instrukcja dotyczy również stażystów, praktykantów, osoby współpracujące na podstawie umów cywilnoprawnych i innych osób mających dostęp danych osobowych.
6. Nieprzestrzeganie postanowień niniejszej instrukcji stanowi naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej określonej przepisami Kodeksy Pracy.
7. Jeżeli skutkiem działania użytkownika jest szkoda materialna, sprawca może ponieść odpowiedzialność materialną na warunkach określonych w przepisach Kodeksy Pracy oraz Kodeksu Cywilnego.

Rozdział II

UPRAWNIENIA DO PRZETWARZANIA DANYCH

§2

1. W przypadku kiedy Administrator nadaje upoważnienie do przetwarzania danych osobowych i obejmuje ono przetwarzanie danych w systemach informatycznych Administrator Systemu Informatycznego (ASI) rejestruje użytkownika w systemie, nadaje mu uprawnienia i szkoli z zakresu bezpieczeństwa korzystania z systemu informatycznego.
2. W systemach informatycznych dla każdego użytkownika osobno w każdym programie rejestrowany jest odrębny identyfikator powiązany ze znanym tylko i wyłącznie użytkownikowi hasłem. Identyfikator jednoznacznie identyfikuje, weryfikuje i autoryzuje tożsamość użytkownika, w szczególności jest podstawą do monitorowania czynności użytkownika w systemie oraz dochodzenia konsekwencji tych czynności.
3. Zalecane jest aby identyfikator składał się z pierwszej litery imienia i nazwiska, pierwszej litery imienia i pełnego nazwiska lub innych oznaczeń umożliwiających identyfikację użytkownika.
4. Identyfikator użytkownika, który utracił uprawnienia nie jest usuwany z systemu informatycznego oraz nie jest przydzielany innej osobie.

Rozdział III

ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

§3

1. Hasło użytkownika nie może być takie samo jak jego identyfikator.
2. ASI przydziela użytkownikowi hasło tymczasowe, które jest przekazywane użytkownikowi w formie ustnej lub pisemnej w sposób, który uniemożliwia zapoznanie się z hasłem przez osoby trzecie.
3. Po zalogowaniu się do systemu za pomocą hasła tymczasowego użytkownik zobowiązany jest do niezwłocznej jego zmiany, chyba że system uniemożliwia wykonanie takiej operacji.
4. Hasło musi się składać z co najmniej z 8 znaków. Wskazane jest, aby zawierało małe i wielkie litery, cyfry oraz znaki specjalne.
5. Użytkownik po pierwszym zalogowaniu się do systemu jest zobowiązany do zmiany hasła.
6. Hasło należy również zmieniać co 30 dni.
7. Użytkownik zobowiązany jest do zabezpieczenia swojego hasła przed nieuprawnionym dostępem osób trzecich.
8. Użytkownik jest zobowiązany do utrzymania swoich haseł w tajemnicy, również po utracie ich ważności.
9. Hasło przy wpisywaniu nie może być w sposób jawny wyświetlane na ekranie.
10. Hasło użytkownika musi być zmienione niezwłocznie w przypadku jego ujawnienia lub podejrzenia ujawnienia.
11. Za zarządzanie hasłami odpowiedzialny jest ASI.
12. ASI musi mieć możliwość zmiany hasła użytkownika bez znajomości aktualnego lub nieważnego hasła użytkownika.
13. Żaden z użytkowników, łącznie z Administratorem nie może mieć możliwości uzyskania z systemu informatycznego aktualnego lub nieważnego hasła innego użytkownika.
14. W pomieszczeniach stanowiących obszar przetwarzania danych, osoby trzecie mogą przebywać wyłącznie w obecności osób upoważnionych do przetwarzania danych.
15. W pomieszczeniach gdzie przyjmowani są klienci, monitory muszą być tak ustawione, aby uniemożliwić osobie nieuprawnionej wgląd w dane.

Rozdział IV

PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZ UŻYTKOWNIKA SYSTEMU

§4

1. Rozpoczęcie i zakończenie pracy systemu informatycznego nadzoruje ASI.
2. ASI ma prawo do monitorowania pracy urządzeń przyłączonych do sieci informatycznej pod kątem przesyłania i przetwarzania danych, rejestracji zdarzeń związanych z przesyłaniem i przetwarzaniem danych w oprogramowaniu oraz prawidłowości wykorzystania powierzonego użytkownikom sprzętu i oprogramowania.
3. Sposób wymiany i przesyłania danych w sieci lokalnej musi umożliwić identyfikację pracujących użytkowników oraz ich działań przy wykorzystaniu sieci informatycznej i oprogramowania.
4. Informacje pozyskane w wyniku monitorowania działań użytkowników oraz pracy urządzeń są dostępne wyłącznie dla Administratora, IOD i ASI, w przypadku uzasadnionej konieczności również dla bezpośrednich przełożonych

użytkownika. Informacje te, mogą zostać wykorzystane wyłącznie do celów służbowych, związanych z bezpieczeństwem przetwarzania danych w systemach informatycznych.

§5

1. Przed przystąpieniem do pracy w systemie informatycznym użytkownik zobowiązany jest sprawdzić urządzenie komputerowe oraz stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych.
2. Użytkownik przed przystąpieniem do przetwarzania danych powinien zalogować się w systemie posługując się swoim identyfikatorem i hasłem.
3. Po upływie 30min bezczynności uruchamiany jest wygaszacz ekranu. Do ponownego wznowienia pracy konieczne jest ponowne zalogowanie się do systemu.
4. Niedopuszczalne jest logowanie się na identyfikator i hasło innego użytkownika lub praca w systemie informatycznym na koncie innego użytkownika.
5. Udostępnianie własnego identyfikatora z hasłem stanowi poważne naruszenie obowiązków pracownika.

§6

1. Jeżeli zachodzi konieczność czasowego opuszczenia stanowiska pracy, przyłączonego do sieci informatycznej lub służącego do przetwarzaniu danych, wiążącego się z utratą z pola widzenia swojego stanowiska pracy, użytkownik zobowiązany jest wykonać jedną z trzech poniższych czynności:
   a) wylogować się z programu lub sieci informatycznej,
   b) zablokować stację roboczą odpowiednią kombinacja klawiszy, przy czym odblokowanie może nastąpić dopiero po podaniu hasła,
   c) aktywować wygaszacz ekranu, w taki sposób aby powrót do pracy był możliwy dopiero po podaniu hasła.
2. Dokumenty nie mogą być pozostawione na biurku podczas nieobecności pracownika.

§7

1. Aby zakończyć pracę w systemie informatycznym użytkownik powinien:
   a) zamknąć wszystkie aktywne programy,
   b) wylogować się z systemu,
   c) wyłączyć urządzenia współpracujące z komputerem tj.: monitor, drukarka, skaner itp.,
   d) wyłączyć komputer,
   e) wyłączyć listwę zasilającą.
2. Wyłączanie komputera w czasie działania programu przyciskiem „Power" lub „Reset" może spowodować trwałe uszkodzenie zbiorów danych.
3. Zabrania się wyłączać przewody zasilające i sieciowe z gniazda elektrycznego.
4. Kończąc pracę na stanowisku należy zabezpieczyć swoje stanowisko pracy (nośniki USB, CD, DVD, dokumenty i wydruki), wyłączyć odbiorniki energii elektrycznej oraz upewnić się, że szafy i biurka z dokumentacja są zamknięte na klucz, a klucz schowany w bezpieczne miejsce.
5. Zakończenie pracy systemu polega na sprawdzeniu czy wszystkie aplikacje sieciowe zostały zamknięte, a następnie wykonanie procedury zamknięcia całego systemu informatycznego.
6. ASI w razie pojawienia się problemów z poprawnym działaniem systemu lub brakiem zasilania elektrycznego, zobowiązany jest do sprawdzenia przyczyn awarii. W przypadku gdy awarii nie da się usunąć w ciągu kilku minut,

powinien on odłączyć systemy sieciowe. Użytkownicy sieciowi w tym przypadku powinni niezwłocznie wyłączyć komputery w kolejności podanej w ust.1.

7. Po awaryjnym przerwaniu pracy komputera, należy sprawdzić czy zostały zapisane ostatnio wprowadzone dane do używanych w tym czasie programów.

8. W pomieszczeniu, w którym znajduje się serwer może pracować tylko ASI oraz osoby przez niego upoważnione. Przebywanie w tym pomieszczeniu osób nieupoważnionych do przetwarzania danych dozwolone jest tylko pod nadzorem ASI.

Rozdział V

PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

§8

1. Kopią zapasową objęte są dane znajdujące się na serwerach sieci informatycznej.

2. Za sporządzenie i bezpieczeństwo kopii zapasowych i awaryjnych odpowiedzialny jest ASI. W wyjątkowych sytuacjach sporządzenie kopii zapasowych i awaryjnych można powierzyć osobie upoważnionej przez ASI w porozumieniu z Administratorem.

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

4. Kopie wykonuje się na nośniku wymiennym, na stacji posiadającej dostęp do danych systemu.

5. Kopia zapasowa wykonywana jest przez kopiowanie całości danych.

6. Kopia całości zasobów przetwarzanych w formie elektronicznej zawierających dane jest wykonywana przez ASI raz na trzy miesiące.

7. Nośniki zawierające kopie zapasowe są przechowywane w szafie zamkniętej na klucz, do której dostęp posiada wyłącznie ASI lub w wyjątkowej sytuacji, osoba przez niego wyznaczona.

8. Po wykonaniu kopii zapasowej ASI ma obowiązek sprawdzić poprawność i kompletność skopiowanych danych oraz zweryfikować możliwość ich przywrócenia.

Rozdział VI

WYDRUKI, ELEKTRONICZNE NOŚNIKI INFORMACJI ZAWIERAJĄCE DANE OSOBOWE ORAZ KOPIE ZAPASOWE

§9

1. Nie należy magazynować zbędnych plików i wydruków.

2. Przeznaczone do likwidacji elektroniczne i optyczne nośniki informacji, mogące zawierać dane osobowe, pozbawia się w sposób trwały zapisu tych danych, a w przypadku gdy nie jest to możliwe, niszczy lub uszkadza się w sposób trwale uniemożliwiający ich odczytanie. Fakt zniszczenia nośników powinien być potwierdzony protokołem.

3. Kopie zapasowe usuwa się niezwłocznie w przypadku ich uszkodzenia lub po utracie terminu przechowywania, w sposób trwale uniemożliwiający ich odczytanie.

4. Za skasowanie zbędnych danych lub zniszczenie zbędnych lub wycofanych z użytku nośników elektronicznych odpowiedzialny jest ASI.

5. Zniszczenie zbędnych lub wycofanych z użytku nośników elektronicznych może być zlecone również firmie zewnętrznej.

6. Za bezpieczeństwo danych zapisanych w komputerach przenośnych oraz w innych urządzeniach przenośnych w całości odpowiada pracownik komputera lub urządzenia przenośnego. Osoba użytkująca komputer przenośny, służący do przetwarzania danych, zobowiązania jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera, w celu zapobiegnięcia dostępu do danych osobie nieupoważnionej, a w szczególności powinna zabezpieczyć dostęp do komputera hasłem i nie zezwalać na użytkowania komputera osobom nieupoważnionym do dostępu do danych, w szczególności komputera nie należy pozostawiać w samochodzie.

7. W przypadku konieczności przekazywania elektronicznych lub optycznych nośników informacji zawierających dane podmiotów zewnętrznych w sytuacjach niezwiązanych z wykonywanymi działaniami służbowymi, nośniki te pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiających ich odzyskanie.

Rozdział VII

ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO

§10

1. System informatyczny jest zabezpieczony przez zastosowanie rozwiązań programowych i sprzętowych np. UPS, listwy przepięciowe.

2. Za aktualność zabezpieczeń, konfigurację, dostosowywanie odpowiedzialny jest ASI.

3. ASI jest zobowiązany zgłaszać Administratorowi wszelkie potrzeby, niedociągnięcia w zakresie zapewnienia bezpieczeństwa systemu informatycznego.

4. W sytuacji, gdy system zabezpieczeń wskazuje zagrożenie, użytkownicy muszą natychmiast powiadomić o tym ASI, który po usunięciu zagrożenia sprawdza system i przywraca go do pełnej funkcjonalności.

5. Użytkownikowi zakazuje się otwierać na komputerach plików pochodzących z niewiadomego źródła bez zgody ASI lub osoby przez niego wyznaczonej.

6. Użytkownikowi zakazuje się samowolnego korzystania z prywatnych lub pochodzących ze źródła innego niż miejsce pracy nośników informacji. Korzystanie z takich nośników może mieć miejsce wyłącznie po uzyskaniu zgody Administratora lub ASI, po uprzednim sprawdzeniu nośnika informacji przez ASI pod względem bezpieczeństwa dla systemu informatycznego.

7. Użytkownikowi zakazuje się wykorzystywania powierzonego im sprzętu informatycznego, oprogramowania oraz dostępu do zasobów informatycznych do jakichkolwiek celów innych niż wykonywanie powierzonych im obowiązków służbowych.

8. Użytkownikowi zakazuje się instalowania na stacjach roboczych jakiegokolwiek oprogramowania z jakiegokolwiek źródła za wyjątkiem aktualizowanych automatycznie komponentów systemu operacyjnego.

9. W przypadku konieczności zainstalowania innego oprogramowania niż to, które otrzymuje do dyspozycji na powierzonej mu stacji roboczej, użytkownik zgłasza taką potrzebę swojemu bezpośredniemu przełożonemu, który

konsultuje się z ASI. W przypadku pozytywnej opinii jedyną osobą uprawnioną do zainstalowania dodatkowego oprogramowania jest ASI.

10. Użytkownikowi zakazuje się łamania lub obchodzenia zabezpieczeń systemów informatycznych. O każdym przypadku znalezienia luki w zabezpieczeniach użytkownik ma obowiązek powiadomić Administratora lub ASI.

11. Użytkownicy są bezpośrednio odpowiedzialni za zainstalowane na powierzonych im stacjach roboczych oprogramowanie i mają prawo zgłaszać wszelkie wątpliwości do ASI, ze szczególnym uwzględnieniem zmian, które zostały wprowadzone podczas ich nieobecności.

12. Za wdrożenie i korzystanie z oprogramowania antywirusowego oraz oprogramowania firewall, a także wszelkich innych mechanizmów obrony systemu informatycznego odpowiedzialny jest ASI.

§11

1. Do ochrony antywirusowej należy stosować program antywirusowy, zainstalowany na komputerze, gdzie odbiera się poczta elektroniczna i sprawdzane są wszystkie nośniki wymienne, przed ich uruchomieniem w sieci oraz na komputerach wolnostojących.

2. Sprawdzanie dostępnymi programami antywirusowymi odbywać się powinno przynajmniej raz w miesiącu.

3. Każdą przesyłkę otrzymaną za pomocą transmisji danych (e-mail, ftp) należy sprawdzić programem antywirusowym. W przypadku wykrycia wirusa choćby na jednym komputerze, należy sprawdzić wszystkie stacje robocze w jednostce.

4. Za ochronę antywirusową odpowiedzialny jest ASI.

Rozdział VIII

PRZEGLĄDY, KONSERWACJA SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

§12

1. Przeglądu i konserwacji sprzętu w sieci informatycznej, systemów informatycznych i nośników informacji dokonuje stosownie do potrzeb ASI w porozumieniu z Administratorem.

2. Zasilacz UPS powinien zapewnić automatyczne zakończenie pracy i wyłączenie serwerów przy zaniku lub nadmiernym wahaniu napięcia (minimalny czas podtrzymywania pracy wynosi ok 5min.).

3. W przypadku przekazywania komputera z dyskiem lub innym nośnikiem danych do naprawy, należy nośnik zdemontować, zabezpieczyć dostęp hasłem lub dokonać naprawy w obecności ASI.

4. W przypadku przekazania nośnika innemu podmiotowi należy dane nieodwracalnie skasować.

5. Użytkownik ma obowiązek niezwłocznie powiadomić IOD oraz ASI o wszelkich nieprawidłowościach i awariach sprzętu informatycznego, mogących prowadzić do próby naruszenia bezpieczeństwa danych.

6. Jeśli urządzenia, dyski lub inne nośniki informacji zawierające dane wymagają naprawy, pozbawia się je wcześniej zapisu danych w sposób uniemożliwiający ich odzyskanie.

7. Zabronione jest dokonywanie napraw sprzętu komputerowego samodzielnie przez użytkowników.

8. Jeśli urządzenia, dyski lub inne nośniki informacji zawierające dane będą poddane likwidacji, pozbawia się je wcześniej zapisanych na nich danych, a w przypadku gdy nie jest to możliwe, uszkadza się jest w sposób uniemożliwiający ich odczytanie.

9. Do wydzielonej strefy energetycznej zasilającej system komputerowy nie wolno podłączać żadnych innych urządzeń tj. czajniki elektryczne, radioodbiorniki czy tez odkurzacze.

Zaakceptował Administrator Danych Osobowych
Dyrektor Domu Pomocy Społecznej dla Kombatantów
w Biłgoraju:

Opracował Inspektor Ochrony Danych:

INSPEKTOR OCHRONY DANYCH
mgr Ewa Kwiecińska
.....

DYREKTOR
mgr Agnieszka Kiesz
.....