Nazwa dokumentu:

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH, ZE SZCZEGÓLNYM UWZGLĘDNIENIEM WYMOGÓW BEZPIECZEŃSTWA INFORMACJI

Numer dokumentu:

DS - 47_e-1

	Imię i nazwisko	Stanowisko	Data	Zarządzenie wprowadzające
Opracował:	Grzegorz Rzepkowski	Informatyk, Administrator Bezpieczeństwa Informacji	27.07.2011r.	Zarządzenie Nr 56/2011 Starosty Pułtuskiego z dnia 27.07.2011 r.
Zatwierdził:	Edward Marek Wroniewski	Starosta Pułtuski	27.07.2011r.	

Spis treści

Rozdział I
Wprowadzenie

1. Podstawę prawną dla opracowania i wdrożenia niniejszej instrukcji stanowią:
    a) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r., nr 101, poz. 926 z póź. zm.);
    b) 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);
2. Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, zwana dalej „instrukcją", jest wewnętrznym dokumentem Administratora Danych Osobowych Starostwa Powiatowego w Pułtusku, skierowanym do osób zatrudnionych przy przetwarzaniu danych osobowych w systemie informatycznym.
3. Dane osobowe gromadzone są w zbiorach danych osobowych Starostwa Powiatowego w Pułtusku i przetwarzane przy wykorzystaniu między innymi systemów informatycznych.
4. Instrukcja dotyczy sieci informatycznej, systemów informatycznych i programów komputerowych za pomocą których można przetwarzać dane, dostępnych w lokalnej sieci komputerowej lub zainstalowanych na poszczególnych stacjach roboczych, zlokalizowanych w budynkach Starostwa Powiatowego w Pułtusku.
5. Wszystkie osoby zatrudnione przy przetwarzaniu danych osobowych w systemach informatycznych bez względu na zajmowane stanowisko i miejsce pracy oraz charakter stosunku pracy są zobowiązane do postępowania zgodnie z zasadami określonymi w niniejszej instrukcji.
6. Polecenia osób wyznaczonych przez administratora danych osobowych do realizacji zadań w zakresie ochrony informacji i bezpieczeństwa systemów informatycznych muszą być bezwzględnie wykonywane przez wszystkich użytkowników.
7. Nieprzestrzeganie postanowień niniejszej instrukcji oraz brak nadzoru nad bezpieczeństwem informacji stanowi naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej określonej przepisami Kodeksu Pracy. Jeżeli skutkiem działania użytkownika jest ujawnienie informacji osobie nieupoważnionej, sprawca może być pociągnięty do odpowiedzialności karnej określonej przepisami Kodeksu Karnego. Jeżeli skutkiem działania użytkownika jest szkoda materialna, sprawca ponosi odpowiedzialność materialną na warunkach określonych w przepisach Kodeksu Pracy oraz Kodeksu Cywilnego.

Rozdział II
Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.

1. Administrator Danych Osobowych za pośrednictwem Administratora Bezpieczeństwa Informacji prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym, zawierającą imię, nazwisko, datę nadania uprawnień, datę ustania uprawnień oraz zakres dostępu.
2. Administrator Bezpieczeństwa Informacji ustala poziom zabezpieczeń obwiązujących w sieci informatycznej i systemach informatycznych.
3. Systemy informatyczne działające w Starostwie Powiatowym w Pułtusku mogą być używane tylko na potrzeby realizacji działań nałożonych na Starostwo Powiatowe w Pułtusku.
4. Dostęp do sieci informatycznej, systemów informatycznych i programów zabezpieczony jest systemem użytkowników i haseł oraz ograniczaniem dostępu do zasobów sieci. Identyfikator i hasło jednoznacznie identyfikują, weryfikują i autoryzują tożsamość użytkownika.
5. Rejestracji użytkowników w systemie dokonuje Administrator Systemu Informatycznego w porozumieniu z Administratorem Bezpieczeństwa Informacji.
6. W systemie informatycznym rejestrowani mogą być wyłącznie użytkownicy, których Administrator Danych Osobowych wpisał do ewidencji osób upoważnionych do przetwarzania danych.
7. W systemach informatycznych dla każdego użytkownika osobno w każdym programie rejestrowany jest odrębny identyfikator powiązany ze znanym tylko i wyłącznie użytkownikowi hasłem.
8. Identyfikator jednoznacznie identyfikuje, weryfikuje i autoryzuje tożsamość użytkownika, a w szczególności jest podstawą do monitorowania czynności użytkownika w systemie oraz dochodzenia konsekwencji tych czynności.
9. Użytkownikom nadawane są uprawnienia do pracy tylko w wymaganych dla realizacji powierzonych zadań modułach i funkcjach programów. Przyznanie, zmiana lub ograniczenie uprawnień następuje na pisemny wniosek przełożonego użytkownika złożony zaakceptowany Administratorowi Danych Osobowych i jest realizowane przez Administratora Systemu Informatycznego – załącznik 1 do niniejszej instrukcji.
10. Wyłączenie użytkownika z ewidencji osób upoważnionych do przetwarzania danych osobowych obliguje Administratora Bezpieczeństwa Informacji w porozumieniu z Administratorem Systemu Informatycznego do odebrania temu użytkownikowi dostępu do danych osobowych przetwarzanych w systemie informatycznym oraz do wyrejestrowania go z wszystkich systemów informatycznych, do których miał uprawnienia.
11. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych nie jest usuwany z systemu informatycznego i nie jest przydzielany innej osobie.
12. Administrator Systemu Informatycznego w każdym momencie musi dysponować wykazem identyfikatorów przyznanych użytkownikom w poszczególnych systemach informatycznych powiązaną z imiennym wskazaniem użytkownika danego identyfikatora. Wykaz ten musi uwzględniać również użytkowników, którym odebrano uprawnienia i wyrejestrowano z systemu.

Rozdział III
Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem.

1. Użytkownik jest w pełnym zakresie odpowiedzialny za swoje hasło, w tym za jego okresowe zmienianie i utrzymywanie w tajemnicy.
2. Użytkownik jest w pełnym zakresie odpowiedzialny za dostosowanie hasła do opisanych niżej obowiązujących reguł, jeśli przestrzegania tych reguł nie wymusza w sposób automatyczny system informatyczny lub oprogramowanie.
3. Żaden z użytkowników, łącznie z Administratorami, nie może mieć możliwości uzyskania z systemu informatycznego aktualnego lub nieważnego hasła innego użytkownika.
4. Administrator Systemu Informatycznego musi mieć możliwość zmiany hasła użytkownika bez znajomości aktualnego lub nieważnego hasła użytkownika.
5. Hasło użytkownika nie może być takie samo jak identyfikator użytkownika.
6. Hasło użytkownika musi składać się z co najmniej 8 znaków, wskazane jest, by zawierało litery, cyfry i znaki specjalne.
7. Hasło użytkownika musi być zmieniane nie rzadziej niż co 30 dni. Hasło użytkownika musi być zmienione niezwłocznie w przypadku jego ujawnienia lub podejrzenia ujawnienia.
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. Hasła Administratora Systemu Informatycznego mogą być znane wyłącznie Administratorowi Bezpieczeństwa Informacji i osobom przez niego upoważnionym. Przechowuje się je w zaklejonej kopercie w zabezpieczonym miejscu. Otwarcie koperty może nastąpić wyłącznie w przypadku uzasadnionej konieczności w porozumieniu z Administratorem Danych Osobowych.

Rozdział IV
Procedury rozpoczęcia, zawieszenia i zakończenia pracy przez użytkowników systemu.

1. Administrator Danych Osobowych ustala okres czasu, w których użytkownicy systemu informatycznego mogą korzystać z jego zasobów. Praca poza tym okresem wymaga zgody Kierownictwa Starostwa Powiatowego w Pułtusku, w formie upoważnienia jednorazowego lub stałego w formie pisemnej.
2. Administrator Bezpieczeństwa Informacji lub Administrator Systemu Informatycznego monitoruje rozpoczęcie i zakończenie pracy systemu informatycznego.
3. Administrator Bezpieczeństwa Informacji lub Administrator Systemu Informatycznego 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.
4. Przed rozpoczęciem pracy w sieci informatycznej użytkownik musi się w niej autoryzować przez podanie swojego identyfikatora i hasła. Dopiero po pomyślnej autoryzacji w sieci informatycznej użytkownik może uruchomić program służący do przetwarzania danych osobowych, dokonując osobnej autoryzacji w tym programie.
5. Sposób wymiany i przesyłania danych w sieci lokalnej musi umożliwiać identyfikację pracujących użytkowników oraz ich działań przy wykorzystaniu sieci informatycznej i oprogramowania.
6. Informacje pozyskane w wyniku monitorowania działań użytkowników oraz pracy urządzeń są dostępne wyłącznie Administratorowi Danych Osobowych, Administratorowi Bezpieczeństwa Informacji i Administratorowi Systemu Informatycznego, w przypadku uzasadnionej konieczności również Lokalnym Administratorom Bezpieczeństwa Informacji, i mogą zostać wykorzystane wyłącznie do celów służbowych, związanych z bezpieczeństwem przetwarzania danych w systemach informatycznych.
7. Kontrola przetwarzanych danych prowadzona jest na bieżąco przez użytkownika na każdym stanowisku merytorycznym. Nadzór prowadzi bezpośredni przełożony użytkownika, Administrator Systemu Informatycznego i Administrator Bezpieczeństwa Informacji.
8. W przypadku konieczności czasowego opuszczenia stanowiska pracy przyłączonego do sieci informatycznej lub służącego przetwarzaniu danych wiążącego się ze stratą z pola widzenia swojego stanowiska, użytkownik powinien: wylogować się z programu lub sieci informatycznej, lub zablokować stację roboczą odpowiednią kombinacją klawiszy, przy czym odblokowanie może nastąpić dopiero po podaniu hasła, uruchomiono konfigurację wygaszacza ekranu, która po 10 minutach bezczynności blokuje stację, powrót do normalnej pracy jest możliwy dopiero po podaniu hasła.
9. Użytkownik jest zobowiązany do zadbania, aby niemożliwe było odczytanie informacji z monitora przez osoby nieuprawnione.
10. Użytkownik jest zobowiązany do wyrejestrowania się z systemu informatycznego przed wyłączeniem stacji roboczej.
11. W sytuacji naruszenia lub podejrzenia naruszenia bezpieczeństwa systemu, użytkownicy zobowiązani są do bezzwłocznego powiadomienia o tym fakcie Lokalnego Administratora Bezpieczeństwa Informacji, Administratora Bezpieczeństwa Informacji lub Administratora Systemu Informatycznego.
12. W pomieszczeniu w którym znajdują się serwery może pracować tylko Administrator Systemu Informatycznego i osoby przez niego upoważnione. Przebywanie w tym pomieszczeniu osób nieupoważnionych do przetwarzania danych osobowych możliwe jest wyłącznie pod nadzorem Administratora Systemu Informatycznego.

Rozdział V
Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

1. Kopią zapasową i awaryjną objęte są dane znajdujące się na serwerach Urzędu oraz dane z wyznaczonych komputerów stacjonarnych.
2. Za sporządzenie i bezpieczeństwo kopii zapasowych i awaryjnych odpowiedzialny jest Administrator Systemu Informatycznego.
3. W wyjątkowych przypadkach sporządzenie kopii zapasowych i awaryjnych można powierzyć osobie upoważnionej przez Administratora Systemu Informatycznego w porozumieniu z Administratorem Bezpieczeństwa Informacji.
4. Harmonogram sporządzania kopii zapasowych musi gwarantować dostępność w każdej chwili kopii: z ostatnich siedmiu dni, z końca ubiegłego miesiąca oraz z końca ubiegłego roku.
5. Kopie dzienne zapisywane są na zewnętrznym dysku twardym znajdującym się pod stałym nadzorem Administratora Systemu Informatycznego i podłączonym bezpośrednio do serwera Urzędu oraz na urządzeniu sieciowym umieszczonym w innym budynku Urzędu podłączonym poprzez sieć wewnętrzna, kopie miesięczne i roczne zapisywane są na nośnikach zewnętrznych, które przechowuje się w szafie metalowej w pomieszczeniu Informatyka Urzędu.
6. Kopie awaryjne tworzone są przed każdą aktualizacją systemu informatycznego, składników systemu informatycznego lub poszczególnych programów służących do przesyłania lub przetwarzania danych. Kopie awaryjne zapisywane są na lokalnym dysku twardym komputera znajdującego się pod stałym nadzorem Administratora Systemu Informatycznego.
7. Użytkownicy we własnym zakresie odpowiadają za sporządzanie kopii zapasowych i awaryjnych wytworzonych przez siebie dokumentów i danych znajdujących się na lokalnych dyskach twardych wykorzystywanych przez nich stacji roboczych, przy jednoczesnym obowiązku dopilnowania, aby dane na lokalnym dysku twardym nie zawierały danych osobowych. Kopie należy zgrywać cyklicznie na dysk sieciowy do imiennego katalogu.
8. W czasie wykonywania kopii zapasowej dostęp do kopiowanych danych dla wszystkich użytkowników jest zablokowany.
9. Po wykonaniu kopii zapasowej i awaryjnej Administrator Systemu Informatycznego ma obowiązek sprawdzić poprawność i kompletność skopiowanych danych oraz zweryfikować możliwość ich przywrócenia i wykorzystania.

Rozdział VI
Sposób, miejsce i okres przechowywania wydruków, elektronicznych nośników informacji oraz kopii zapasowych zawierających dane osobowe.

1. Wydruki archiwalne lub bieżące przechowywane mogą być wyłącznie w pomieszczeniach uniemożliwiających dostęp do nich przez osoby nieupoważnione.
2. Kopie zapasowe na nośnikach przechowywane są w zamkniętej szafie metalowej, do której dostęp mają wyłącznie osoby upoważnione przez Administratora Bezpieczeństwa Informacji oraz Administrator Systemu Informatycznego.
3. Za bezpieczeństwo danych zapisanych w komputerach przenośnych oraz w innych urządzeniach przenośnych w całości odpowiada użytkownik komputera lub urządzenia przenośnego.
4. Zbędne wydruki zawierające dane osobowe natychmiast po wykorzystaniu muszą zostać zniszczone w niszczarce dokumentów.
5. Przeznaczone do likwidacji nośniki informacji (m.in. elektroniczne, magnetyczne i optyczne), 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 – *protokół zniszczenia nośnia stanowi załącznik nr 2 do niniejszego dokumentu.*
6. Kopie zapasowe usuwa się niezwłocznie w wypadku ich uszkodzenia lub po utracie terminu przechowywania, w sposób trwale uniemożliwiający ich odczytanie.
7. Za zniszczenie zbędnych wydruków i innych zbędnych dokumentów zawierających dane osobowe odpowiedzialny jest Dyrektor Wydziału.
8. Za skasowanie zbędnych danych lub zniszczenie zbędnych nośników elektronicznych odpowiedzialny jest Administrator Systemu Informatycznego.
9. Kopie zapasowe przechowuje się przez okres:
    a. dzienne - przez siedem dni,
    b. tygodniowe, miesięczne - dwunastu miesięcy następujących po miesiącu sporządzenia kopii, dopuszcza się dłuższy okres przechowywania, o ile pozwalają na to warunki,
    c. roczne - nieograniczony.
10. W przypadku konieczności przekazywania elektronicznych lub optycznych nośników informacji zawierających dane osobowe podmiotom zewnętrznym w sytuacjach nie związanych z wykonywanymi działaniami służbowymi, nośniki te pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie.
11. W przypadku konieczności przewiezienia elektronicznych lub optycznych nośników informacji zawierających dane osobowe pomiędzy budynkami Starostwa Powiatowego w Pułtusku lub innymi instytucjami – Administrator Bezpieczeństwa Informacji dokonuje tego zapewniając maksymalne bezpieczeństwo danych (może również posiłkować się eskortą w postaci Policji, Straży Miejskiej czy Agencji Ochrony).

Rozdział VII
Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego lub inna ingerencja w ten system.

1. System informatyczny jest zabezpieczany przez zastosowanie rozwiązań sprzętowych i programowych *(m.in. urządzenia UTM na styku Internet/sieć wewnętrzna, programy antywirusowe)*.
2. Za aktualność stosowanych zabezpieczeń, dostosowywanie do aktualnych potrzeb, konfigurację i zarządzanie nimi odpowiada Administrator Systemu Informatycznego.
3. Administrator Systemu Informatycznego ma obowiązek zgłaszać na piśmie Administratorowi Danych Osobowych wszelkie potrzeby lub zauważone niedociągnięcia w zakresie zapewnienia bezpieczeństwa systemu informatycznego.
4. Wykorzystywane rozwiązania muszą zapewnić automatyczne działania w przypadku wykrycia zagrożenia w systemie informatycznym oraz zapewnić możliwość konfiguracji odpowiednio do potrzeb.
5. W przypadku, gdy system zabezpieczeń wskazuje zaistnienie zagrożenia, użytkownicy są zobowiązani bezzwłocznie powiadomić o tym fakcie Administratora Systemu Informatycznego, który po jego usunięciu sprawdza system i przywraca go do pełnej funkcjonalności.
6. Dla minimalizacji zagrożeń należy dążyć do maksymalnej unifikacji sprzętu działającego w systemie informatycznym, stosowanego oprogramowania, konfiguracji sprzętu i oprogramowania, a także rozwiązań organizacyjnych.
7. Bezwzględnie zakazuje się użytkownikom samowolnego korzystania z prywatnych lub pochodzących ze źródła innego niż miejsce pracy nośników informacji (m.in. magnetycznych, optycznych, urządzeń podłączanych do stacji roboczych). Korzystanie z takich nośników może mieć miejsce wyłącznie po uzyskaniu zgody Administratora Bezpieczeństwa Informacji lub Administratora Systemu Informatycznego, po uprzednim sprawdzeniu nośnika informacji przez Administratora Systemu Informatycznego pod względem bezpieczeństwa dla systemu informatycznego.
8. Bezwzględnie zakazuje się użytkownikom wykorzystywania powierzonego im sprzętu informatycznego, oprogramowania i dostępu do zasobów informatycznych do jakichkolwiek celów innych niż wykonywanie powierzonych im obowiązków służbowych lub związanych z własną edukacją i dokształcaniem.
9. Bezwzględnie zakazuje się użytkownikom samowolnego instalowania na stacjach roboczych jakiegokolwiek oprogramowania z jakiegokolwiek źródła, za wyjątkiem aktualizowanych automatycznie komponentów systemu operacyjnego lub posiadanego oprogramowania.
10. W przypadku konieczności zainstalowania innego oprogramowania niż to, które otrzymuje użytkownik do dyspozycji na powierzonej mu stacji roboczej, obowiązuje Zarządzenie Nr 34/07 Starosty Pułtuskiego z dnia 24 lipca 2007 roku w sprawie Regulaminu użytkowania oprogramowania i sprzętu komputerowego.
11. Bezwzględnie zabrania się użytkownikom łamania lub obchodzenia zabezpieczeń systemów informatycznych. O każdym przypadku znalezienia luki w zabezpieczeniach użytkownik ma obowiązek powiadomić Administratora Bezpieczeństwa Informacji oraz Administratora Systemu Informatycznego.
12. Użytkownicy są bezpośrednio odpowiedzialni za zainstalowane na powierzonych im stacjach roboczych oprogramowanie oraz mają obowiązek zgłaszać wszelkie wątpliwości w tym zakresie Administratorowi Bezpieczeństwa Informacji lub Administratorowi Systemu Informatycznego, ze szczególnym uwzględnieniem zmian, które zostały wprowadzone podczas ich nieobecności.

Rozdział VIII
Sposób odnotowania przez system informatyczny informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia.

Dokładna kopia danych osobowych przesłanych do Zakładu Ubezpieczeń Społecznych przechowywana jest w bazie danych programu Płatnik w postaci dokumentów i zestawów dokumentów oznaczonych odpowiednim statusem dokumentu lub zestawu, datą utworzenia dokumentu, datą wysłania zestawu, identyfikatorem osoby tworzącej zestaw i numerem zestawu.

Rozdział IX
Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

1. Przeglądu i konserwacji sprzętu w sieci informatycznej, systemów informatycznych i nośników informacji dokonuje stosownie do potrzeb Administrator Systemu Informatycznego w porozumieniu z Administratorem Bezpieczeństwa Informacji.
2. W przypadku przekazywania stacji roboczej z dyskiem albo innych nośników informacji do naprawy, dysk lub nośnik jest demontowany, pozbawiany wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie lub naprawa dokonywana jest w obecności osoby upoważnionej przez Administratora Danych Osobowych.
3. Bezwzględnie zabronione jest samodzielne dokonywanie przez użytkowników napraw sprzętu informatycznego, wymiana jego podzespołów oraz wykonywanie innych czynności nie związanych bezpośrednio z jego eksploatacją lub nie dopuszczonych do wykonywania przez producenta sprzętu w instrukcji obsługi.
4. Użytkownik ma obowiązek niezwłocznie powiadomić Administratora Bezpieczeństwa Informacji o wszelkich nieprawidłowościach i awariach sprzętu informatycznego, mogących prowadzić do próby naruszenia lub naruszenia bezpieczeństwa danych osobowych.
5. W przypadku awarii systemu informatycznego i utraty informacji lub w przypadku zaistnienia możliwości uszkodzenia informacji Administrator Systemu Informatycznego w porozumieniu z Administratorem Bezpieczeństwa Informacji jest zobowiązany do:
    a) przetestowania sieci informatycznej, systemu informatycznego oraz aplikacji służącej do przetwarzania danych,
    b) ocenić zasadność odtworzenia danych przy wykorzystaniu aktualnej kopii zapasowej lub kilku kopii zapasowych,
    c) w przypadku uzasadnionej konieczności odtworzyć dane przy wykorzystaniu aktualnej kopii zapasowej lub kilku kopii zapasowych