ZARZĄDZENIE Nr 36/2011

STAROSTY MYŚLIBORSKIEGO

z dnia 12 maja 2011 roku

w sprawie instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych „Pojazd i Kierowca”

Na podstawie art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (tj. Dz. U z 2001 r. Nr 142, poz. 1592 z późn. zmianami) oraz art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zmianami) i § 3 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024), zarządzam, co następuje:

§1. Zatwierdzam i wprowadzam ***Instrukcję określającą sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych „Pojazd i Kierowca”***, która stanowi załącznik do niniejszego zarządzenia.

§2. Wyznaczam Pana Krzysztofa Adamowicza Lokalnym Administratorem Systemu Informatycznego Pojazd i Kierowca.

§3. Wykonanie zarządzenia powierzam Naczelnikowi Wydziału Komunikacji oraz Lokalnemu Administratorowi Systemu Informatycznego Pojazd i Kierowca.

§4. Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik
do Zarządzenia Nr 36/2011
Starosty Myśliborskiego
z dnia 12.05.2011r.

INSTRUKCJA
określająca sposób zarządzania systemem informatycznym służącym do przetworzenia danych osobowych „Pojazd i Kierowca" w Starostwie Powiatowym w Myśliborzu.

§ 1
Postanowienia ogólne.

1. Instrukcja określa sposób zarządzania systemem informatycznym Pojazd i Kierowca w zakresie przetwarzania danych osobowych oraz realizuje wymagania zawarte w § 3 Rozporządzenia 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.
2. W sprawach nie określonych w instrukcji stosuje się postanowienia Instrukcji Bezpieczeństwa Systemu „Pojazd" i „Kierowca" w Urzędzie, Politykę Bezpieczeństwa Systemów Informatycznych oraz Instrukcję Zarządzania Systemami Informatycznymi w Starostwie Powiatowym w Myśliborzu wprowadzoną Zarządzeniem Nr 21/2011 Starosty Myśliborskiego z dnia 21 marca 2011 r.
3. Przez użyte w instrukcji skróty rozumie się:
    1) UODO – ustawa z dnia 29 stycznia 1997 r. o ochronie danych osobowych;
    2) ADO – Administrator Danych Osobowych – Starosta;
    3) ABI – Administrator Bezpieczeństwa Informacji – pracownik który nadzoruje przestrzeganie zasad ochrony danych osobowych;
    4) RMSWiA – 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;
    5) PBSI – Polityka Bezpieczeństwa Systemu Informatycznego;
    6) IBSPiK – Instrukcja Bezpieczeństwa Systemów „Pojazd" i „Kierowca" w Urzędzie;
    7) Administrator Systemu – osoba zarządzająca bieżącą pracą systemu;
    8) Użytkownik systemu:
        - osoba zatrudniona przy przetwarzaniu danych osobowych w Starostwie, która posiada upoważnienie do obsługi systemu a także

osoba wykonująca umowę cywilnoprawną zawartą ze Starostą na przetwarzanie danych osobowych,

- pracownik innego podmiotu, który świadczy usługi związane z funkcjonowaniem systemu np. serwisant.

§ 2

Ochrona zasobów

1. Ochrona zasobów danych osobowych przetwarzanych w tym systemie jest podstawowym obowiązkiem każdego pracownika Wydziału mającego status użytkownika systemu przed ich nieuprawnionym użyciem, zniszczeniem, utratą.
2. Pracownik wydziału mający status użytkownika systemu jest zobowiązany do zachowania w tajemnicy służbowej informacji i wiedzy dotyczącej gromadzenia, przetwarzania oraz ochrony danych osobowych w Wydziale.
3. Obowiązek, o którym mowa w ust. 2 istnieje również po ustaniu zatrudnienia.
4. Obowiązek ten potwierdza każdy pracownik pisemnym oświadczeniem, które jest przechowywane w jego aktach osobowych.

§ 3

Wymagania stawiane systemowi

1. Stosowany system informatyczny, w którym przetwarzane są dane osobowe w starostwie spełnia wymogi określone w RMSWiA oraz przyjętej Polityce Bezpieczeństwa Starostwa.
2. System informatyczny zapewni każdej osobie, której dane są przetwarzane automatyczne odnotowanie:
    1) daty pierwszego wprowadzenia danych osobowych, identyfikatora użytkownika, który wprowadził dane, źródła danych jeżeli jest ich więcej niż jedno, sporządzenia i wydrukowania raportu danych osobowych,
    2) informacji komu i kiedy oraz w jakim zakresie zostały udostępnione dane w rozumieniu art. 7 pkt 6 UODO.
3. System pracuje w produkcyjnej, dedykowanej sieci teleinformatycznej. Przez sieć produkcyjną rozumie się sieć odseparowaną, tj. bez bezpośredniego lub pośredniego połączenia z Internetem i z ograniczonym zarządzalnym połączeniem z innymi sieciami produkcyjnymi.
4. Dane osobowe mogą być przetworzone na komputerach przenośnych wtedy gdy systemy plików na dyskach twardych są szyfrowane, a dostęp do klucza kryptograficznego jest autoryzowany za pomocą hasła, tokenu lub certyfikatu elektronicznego.
5. Pliki zawierające dane osobowe mogą być przesyłane łączami publicznymi gdy zostaną wcześniej zaszyfrowane.

6. System informatyczny uniemożliwia użytkownikowi dostęp do BIOS-u.
7. Korzystanie z nośników wymiennych podlega ograniczeniu i wcześniejszej autoryzacji tego nośnika, przez informatyka Starostwa.
8. Do szyfrowania wymienionego w pkt 6 i 7 stosuje się algorytm AES o długości klucza co najmniej 256 bitów.
9. Do wyliczania skrótów kryptograficznych stosuje się jednokierunkową funkcję SHA – 1.
10. Pomieszczenia serwerowi są chronione za pomocą:
    1) elektronicznego systemu kontroli wykrywania włamań,
    2) elektronicznego systemu wykrywania pożaru,
    3) serwery zaopatrzone są w urządzenia podtrzymujące napięcie UPS.
11. Pomieszczenia, w których eksploatowany jest system informatyczny są chronione przed dostępem osób nieuprawnionych z użyciem:
    1) elektronicznego systemu wykrywania włamań,
    2) elektronicznego systemu wykrywania pożaru.
12. Pomieszczenia w których są gromadzone i przetwarzane dane osobowe oraz przyjmowani są interesanci stosuje się szczególne środki ostrożności, w tym:
    1) oddzielenie części urzędniczej od części dla interesantów przez ustawienie mebli, wykonanie zapór,
    2) umieszczenie kartotek, szaf z aktami w części przeznaczonej dla urzędników oraz takie ich ustawienie by był utrudniony dostęp do tych kartotek,
    3) wchodzenie do pomieszczenia takiej liczby interesantów jaka jest czynna liczba stanowisk – wchodzenie pojedyncze. Interesant pozostaje w pomieszczeniu tylko w obecności pracownika,
    4) dokumenty papierowe, nośniki elektroniczne są składane poza biurkiem tak aby dostęp osób postronnych był utrudniony. Na biurku są tylko akta dotyczące obsługiwanego interesanta,
    5) nie pozostawianie dokumentów, nośników elektronicznych na biurkach, stołach, który umożliwiałby wgląd w nie osób nieuprawnionych,
    6) w części pomieszczeń przeznaczonej dla użytkownika systemu może przebywać, administrator danych, administrator bezpieczeństwa informacji, administrator lokalny lub serwisant w obecności użytkownika systemu. Inni pracownicy nie mają wstępu do tych części pomieszczeń,
    7) monitory używanego sprzętu komputerowego ustawione w ten sposób, że zawartość wyświetlanego ekranu jest niedostępna dla osób nieuprawnionych.
    8) osoby przetwarzające dane osobowe są okresowo szkolone z zasad pracy w systemie, obowiązujących przepisów, Polityki Bezpieczeństwa Starostwa. Osoby

szkolone potwierdzają własnym podpisem fakt odbycia szkolenia. Ze szkoleń zewnętrznych pracownik przekazuje zaświadczenie o odbytym przeszkoleniu.

§ 4

Przyznawanie praw dostępu do systemu.

1. Dostęp do pomieszczeń i systemu, w którym przetwarzane są dane osobowe jest przyznawany pisemnie osobom uprawnionym do przetwarzania danych osobowych, które formalnie zobowiązały się do:
   1) zachowania w tajemnicy przetwarzanych danych osobowych oraz informacji dotyczących środków ich przetwarzania,
   2) niewykraczanie poza przyznane uprawnienia.
2. Tworzenie kont, zmiany lub zawieszenie praw dostępu do systemu dla pracowników Starostwa są realizowane przez Polską Wytwórnię Papierów Wartościowych SA w Warszawie, zgodnie z procedurami zapisanymi w IBSPiK na podstawie pisemnego wniosku Naczelnika Wydziału Komunikacji.
3. Pracownik przetwarzający dane osobowe w tym systemie potwierdza własnoręcznym podpisem zapoznanie się z indywidualnym zakresem czynności dotyczącym przetwarzania danych. Pracownik podlega szkoleniu w zakresie ochrony danych osobowych gromadzonych i przetwarzanych w systemie.
4. Pracownik otrzymuje pisemne upoważnienie do obsługi systemu w zakresie gromadzenia i przetwarzania danych osobowych podpisane przez Administratora Danych.
5. O zmianie odsunięcia lub dopuszczenia pracownika jako użytkownika systemu Administrator Lokalny zawiadamia niezwłocznie Administratora Bezpieczeństwa Informacji.
6. Po otrzymaniu uprawnień dostępu do systemu Administrator Lokalny przekazuje nadany login Administratorowi Bezpieczeństwa Informacji.

§ 5

Uwierzytelnienie w systemie.

1. W systemie stosuje się uwierzytelnienie z użyciem imiennego certyfikatu x 509 √ 3 przechowywanego na karcie kryptograficznej.
2. Certyfikat użytkowania jest wystawiany w Punkcie Rejestracji CCiGKw PWPW SA.
3. Uwierzytelnienie z użyciem identyfikatora i hasła stosuje się wyłącznie w sytuacjach awaryjnych systemu informatycznego określonych w IBSPiK.
4. Hasła te przechowywane są w postaci zaszyfrowanej.
5. W systemie stosuje się hasła na poziomie złożoności określonym w zabezpieczeniu nr VIII załącznika do RMSWiA.
6. System jest tak zaplanowany, że nie zezwala na ustawienie:

1) hasła krótszego niż 8 znaków,
2) kodu PIN do karty nie krótszego niż 4 znaki.

7. System uniemożliwia uwierzytelnienie użytkownika przez 30 min jeżeli trzy kolejne próby uwierzytelnienia zakończyły się niepowodzeniem.
8. Hasło i kod PIN są tworzone i przeznaczone wyłącznie do wiadomości użytkownika i nie powinny być ujawniane osobom trzecim.
9. Wprowadza się wyjątki do opisanej w ust. 8 zasady:
    1) tymczasowy kod PIN karty użytkownika może być znany Administratorowi Systemu PWPW SA bezpośrednio po odblokowaniu karty na wniosek użytkownika,
    2) awaryjne hasło użytkownika Systemów Pojazd i Kierowca jest czasowo przechowywane w PWPW SA gdzie generowane są listy haseł logowania awaryjnego.
10. Hasła i kody PIN w stosunku do których zaistniało podejrzenie ich ujawnienia podlegają niezwłocznej zmianie zgodnie z zasadami określonymi w IBSPiK.
11. Użytkownik systemu, któremu po zablokowaniu karty Administrator Systemu PWPW nadał tymczasowy kod PIN dokonuje niezwłocznie zmianę kodu PIN.
12. PWPW niezwłocznie niszczy kopie list haseł logowania awaryjnego po uzyskaniu potwierdzenia dostarczenia ich do Starostwa.

§ 6

Rozpoczęcie, zawieszenie i zakończenie pracy użytkownika.

1. Użytkownik systemu rozpoczyna pracę od uwierzytelniania się w systemie operacyjnym. W tym, celu wprowadza hasło i kod PIN. Czynności te wykonuje w sposób uniemożliwiający ujawnienie lub podejrzenie ich przez innych pracowników lub osoby trzecie.
2. W przypadku braku możliwości rozpoczęcia pracy lub podejrzeń, że z konta mogły korzystać inne osoby bądź stwierdza, że zostało nienaruszone bezpieczeństwo systemu powiadamia niezwłocznie operatora Infolinii tel. 0 801 300 403 lub Zespół Bezpieczeństwa PWPW SA, tel. (022) 53 02 334 i postępuje wg uzyskanych wskazówek.
3. Użytkownik systemu przetwarzający dane osobowe ustawia monitor pod takim kątem widzenia by podgląd ekranu był niemożliwy przez osoby postronne.
4. Użytkownik przed opuszczeniem stanowiska pracy zabezpiecza stację roboczą przed dostępem osób trzecich aktywując wygaszasz ekranowy zabezpieczony hasłem.
5. Wymieniony wygaszasz ekranu jest aktywizowany automatycznie po 20 min od niewykorzystywania stacji.

6. Każdorazowo użytkownik po zakończeniu pracy w systemie wylosowuje się z systemu.
7. Wydruki robocze papierowe zawierające dane osobowe są niszczone w pomieszczeniu, w którym zostały wytworzone. Niszczenia dokonuje się w niszczarce. Niszczarki używane do tego celu spełniają wymogi klasy S-3 lub wyższej.

§ 7

Wykonywanie kopii bezpieczeństwa.

1. Wykonywanie, przechowywanie i likwidacja kopii bezpieczeństwa odbywa się zgodnie z zadaniami określonymi w IBSPiK.
2. PWPW odpowiada za inicjowanie, wykonywanie i weryfikację poprawności zapisu kopii na nośnikach.
3. Wyznaczony pracownik Wydziału odpowiada za poprawne oznaczenie nośników, ich wymianę w napędzie zgodnie z opisem oraz przechowywanie tych nośników w szafie metalowej poza lokalizacją serwera.
4. Po upływie 3 miesięcy od wycofania z użycia nośników, na których zapisywano kopie bezpieczeństwa dokonuje się niszczenia tych nośników. Niszczenia dokonuje wyznaczony pracownik Wydziału.

§ 8

Elektroniczne nośniki informacji

1. Elektroniczne nośniki danych używane w Systemie Pojazd i Kierowca, na których są gromadzone dane osobowe są przechowywane w pomieszczeniach Wydziału oraz w serwerowni systemu. Pomieszczenia te są zabezpieczone systemami:
    1) elektronicznego wykrywania włamań,
    2) elektronicznego wykrywania pożaru.
2. Wprowadzenie i wycofanie z użycia elektronicznych nośników informacji zainstalowanych na dyskach twardych stacji i serwera odbywa się zgodnie z PBSI.
3. Zabrania się kopiowania danych osobowych z systemu na dodatkowe nośniki z wyjątkiem sporządzonych kopii bezpieczeństwa.

§ 9

Ochrona przed szkodliwym oprogramowaniem.

1. Ochroną przed szkodliwym oprogramowaniem zapewnia się przez zainstalowanie oprogramowania antywirusowego na serwerze i stacjach roboczych.
2. Instalację, aktualizację oraz poprawność działania programów antywirusowych wykonuje PWPW.
3. Oprogramowanie antywirusowe i bazy sygnatur szkodliwego oprogramowania są aktualizowane okresowo przez PWPW zgodnie z określonymi wymaganiami PBSI.

§ 10

Konserwacja i naprawy systemu.

1. Przeglądy, konserwacje i naprawy elementów infrastruktury technicznej systemu i oprogramowania dokonuje PWPW wg zasad określonych w IBSPiK.
2. Prace serwisantów wykonywane są pod nadzorem pracownika Starostwa.
3. Jeżeli wykonanie czynności serwisowych wymaga dostępu do danych osobowych to serwisant zobowiązany jest do podpisania zobowiązania o zachowaniu poufności.
4. Urządzenia komputerowe, dyski twarde lub inne nośniki danych przeznaczone do naprawy poza Starostwem pozbywa się zapisów danych osobowych z tych urządzeń.
5. Wymieniony sprzęt w ust. 4 może być naprawiony pod nadzorem pracownika Starostwa i nie wymaga wtedy usuwania danych osobowych.

§ 11

Postanowienia końcowe.

1. Przestrzeganie i stosowanie niniejszej instrukcji stanowi podstawę do bezpiecznego posługiwania się tym systemem w Starostwie.
2. Instrukcję tą należy stosować równolegle z Instrukcją Bezpieczeństwa Systemu „Pojazd" i „Kierowca" wydaną przez PWPW.
3. Procedury nie opisane w instrukcji a zawarte w Instrukcji Bezpieczeństwa Systemu Informatycznego stosuje się równolegle.

§ 12

Administrator Bezpieczeństwa Informacji Starostwa ma prawo monitorować przestrzeganie przez pracowników systemu przepisów o ochronie danych osobowych.

§ 13

Lokalny administrator realizuje zadania w imieniu Administratora Danych Osobowych.