Załącznik nr 3
do Zarządzenia nr .....
Starosty Ząbkowickiego
z dnia .....

Instrukcja zarządzania systemem informatycznym Pojazd i Kierowca w Starostwie Powiatowym w Ząbkowicach Śląskich

Opracował: Kierownik Wydziału Komunikacji
przy udziale Administratora Bezpieczeństwa Informacji

Ząbkowice Śląskie 2009 r.

SPIS TREŚCI:

I. Postanowienia ogólne

1. Instrukcja określa sposób zarządzania lokalnym systemem informatycznym Pojazd i Kierowca w zakresie przetwarzania danych osobowych i realizuje wymaganie, o którym mowa w § 3 ust.1 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 z późn. zm.).
2. W sprawach nieokreślonych niniejszą instrukcją należy stosować postanowienia Instrukcji Bezpieczeństwa Systemu Pojazd i Kierowca w Urzędzie, oraz Polityki bezpieczeństwa przetwarzania danych osobowych i Instrukcji zarządzania systemami informatycznymi Starostwa Powiatowego w Ząbkowicach Śląskich.
3. Przez użyte w instrukcji określenia należy rozumieć:
   - UODO – ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U.z 2002 r. Nr 101 poz. 926 z późn. zm.),
   - RMSWiA – Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r,
   - IBSPiK – Instrukcja Bezpieczeństwa Systemu Pojazd w Urzędzie i Instrukcja Bezpieczeństwa Systemu Kierowca w Urzędzie,
   - PB – Polityka bezpieczeństwa przetwarzania danych osobowych w Starostwie Powiatowym w Ząbkowicach Śląskich,
   - IZSI – Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Starostwie Powiatowym w Ząbkowicach Śląskich
   - URZĄD – należy rozumieć Starostwo Powiatowe w Ząbkowicach Śląskich,
   - PWPW S.A. – Polska Wytwórnia Papierów Wartościowych S.A
   - ADO – Administrator Danych Osobowych – decyduje o celach i środkach przetwarzania danych osobowych – należy przez to rozumieć Starostę Ząbkowickiego,
   - ABI – Administrator Bezpieczeństwa Informacji – osoba, która nadzoruje przestrzeganie zasad ochrony danych osobowych, powołana przez ADO.

II. Wymagania stawiane systemowi

1. System informatyczny (system), w którym są przetwarzane dane osobowe musi spełniać wymagania określone w RMSWiA.
2. W szczególności system zapewnia dla każdej osoby, której dane osobowe są w nim przetwarzane automatyczne odnotowanie:
    1) daty pierwszego wprowadzenia danych; identyfikatora użytkownika, który wprowadził dane; źródła danych, jeżeli może ich być więcej niż jedno; możliwość sporządzenia i wydrukowania raportu o danych osobowych,
    2) informacji o tym, komu, kiedy i w jakim zakresie zostały udostępnione dane.
3. System pracuje w produkcyjnej, dedykowanej sieci teleinformatycznej.
4. Przez sieć produkcyjną, o której mowa w ust. 3 rozumie się sieć odseparowaną, tj. bez bezpośredniego lub pośredniego (tj. za pośrednictwem innych sieci) połączenia z Internetem i z ograniczonym, zarządzanym połączeniem z innymi sieciami produkcyjnymi.
5. System uniemożliwia użytkownikom dostęp do ustawień BIOS.
6. Korzystanie z nośników wymiennych podlega ograniczeniom i autoryzacji.
7. Pomieszczenia, w których eksploatowany jest system są chronione przed dostępem osób nieuprawnionych

III. Przyznawanie praw dostępu do systemu

1. Dostęp do pomieszczeń i systemu, w którym przetwarzane są dane osobowe jest przyznawany osobom pisemnie upoważnionym do przetwarzania danych osobowych, które formalnie zobowiązują się do:
    1) zachowania w tajemnicy przetwarzania danych osobowych oraz informacji dotyczących środków ich przetwarzania;
    2) niewykraczania poza uprawnienia przyznane w systemie.
2. Tworzenie konta, zmiana lub zawieszenie praw dostępu w systemie dla użytkowników są realizowane przez PWPW S.A. zgodnie z procedurami określonymi w IBSPiK na formalny wniosek osoby upoważnionej przez Urząd.

IV. Uwierzytelnianie w systemie

1. W systemie stosuje się uwierzytelnianie z użyciem imiennego certyfikatu przechowywanego na karcie kryptograficznej.
2. Certyfikaty użytkowników są wystawiane w punkcie Rejestracji CCiGK w PWPW S.A..
3. Uwierzytelnienie z użyciem identyfikatora i hasła jest stosowane wyłącznie w sytuacjach awaryjnych uwzględnionych w IBSPiK.
4. Hasła są przechowywane w postaci zaszyfrowanej.
5. Systemy nie zezwalają na ustanowienie kodu PIN do karty o długości krótszej niż 4 znaki, ale należy stosować PIN o długości minimum 8 znaków.
6. Systemy uniemożliwiają uwierzytelnienie użytkownika przez 30 minut, jeśli trzy kolejne próby uwierzytelniania zakończyły się niepowodzeniem.
7. Hasło i kod PIN są informacjami przeznaczonymi wyłącznie do wiadomości użytkownika systemu i nie powinny być ujawniane osobom trzecim.

V. Rozpoczęcie, zawieszenie i zakończenie pracy użytkownika

1. Rozpoczynając pracę w systemie użytkownik uwierzytelnia się w systemie operacyjnym. Wprowadzenie hasła lub kodu PIN musi odbywać się w sposób uniemożliwiający ich ujawnienie innym osobom.
2. W przypadku braku możliwości rozpoczęcia pracy lub podejrzeń, że z konta użytkownika mogła korzystać inna osoba bądź nastąpiło inne naruszenie bezpieczeństwa systemu należy niezwłocznie powiadomić operatora Infolinii (tel. 0801-300-403) lub bezpośrednio zespół bezpieczeństwa w PWPW S.A (tel. 022 53 02 334) oraz Administratora Bezpieczeństwa Informacji.
3. Ustawienie monitora lub zastosowanie filtra ograniczającego kąt widzenia powinno uniemożliwić podgląd ekranu osobom nieupoważnionym do przetwarzania danych osobowych.
4. W przypadku konieczności czasowego opuszczenia stanowiska pracy, użytkownik systemu obowiązany jest uniemożliwić dostęp do stacji roboczej aktywując wygaszasz ekranowy zabezpieczony hasłem.

5. Zabezpieczenie, o którym mowa w ust. 4 jest aktywowane automatycznie, jeśli stacja robocza przechodzi w stan bezczynności i zostało skonfigurowane przez PWPW S.A. zgodnie z procedurami określonymi w IBSPiK i nie posiada możliwości modyfikacji przez użytkownika.
6. Po zakończeniu pracy przy przetwarzaniu danych osobowych użytkownik powinien wylogować się z systemu.

VI. Kopie bezpieczeństwa

1. Wykonywanie, przechowywanie i likwidacja kopii bezpieczeństwa powinny być realizowane zgodnie z zasadami określonymi w IBSPiK.
2. PWPW S.A odpowiada za inicjowanie, wykonanie i weryfikację poprawności zapisu na nośnikach.
3. Urząd odpowiada za jednoznaczne oznaczenie nośników; ich wymianę w napędzie zgodnie z ustalonym harmonogramem oraz za przechowywanie nośników w miejscu oddalonym od miejsca, w którym jest zlokalizowany serwer i w sposób uniemożliwiający nieuprawnione przejęcie, odczyt, modyfikację, uszkodzenie lub zniszczenie.
4. Ponadto Urząd odpowiada za niszczenie nośników stosowanych do wykonywania kopii bezpieczeństwa po ich wycofaniu z użycia zgodnie z IBSPiK. Ze zniszczenia nośników sporządza się stosowny protokół.

VII. Elektroniczne nośniki informacji

1. Elektroniczne nośniki informacji zawierające dane osobowe powinny być przechowywane w pomieszczeniach uniemożliwiających dostęp osób nieupoważnionych.
2. Nośniki, o których mowa w ust. 1 powinny być przechowywane w sposób uniemożliwiający nieuprawnione przejęcie, odczyt, modyfikacje, uszkodzenie lub zniszczenie;
3. Nośniki elektroniczne powinny być pozbawiane zapisanych na nich danych lub fizycznie niszczone niezwłocznie po ustaniu celu, w jakim dane zostały na nich zapisane.

4. Niszczenie elektronicznych nośników informacji zawierających dane osobowe powinno się odbywać w oparciu o zapisy IZSI.
5. Nieuzasadnione kopiowanie danych osobowych na nośniki jest zabronione.

VIII. Ochrona przed szkodliwym oprogramowaniem

Ochrona przed szkodliwym oprogramowaniem jest realizowana przez oprogramowanie antywirusowe instalowane na serwerach i stacjach roboczych. Instalacji i konfiguracji oprogramowania dokonuje PWPW S.A. zgodnie z procedurami określonymi w IBSPiK i Urząd nie posiada możliwości jej modyfikacji.

IX. Konserwacja i naprawa systemu

1. Przeglądy, konserwacja i naprawy elementów infrastruktury technicznej systemu i oprogramowania są wykonywane przez PWPW S.A. zgodnie z zasadami określonymi w IBSKiK.
2. Praca osób wykonujących czynności serwisowe jest wykonywana pod nadzorem pracownika Urzędu.
3. Jeżeli wykonanie czynności serwisowych wymaga dostępu do danych osobowych to pracownik firmy zewnętrznej jest zobowiązany do podpisania zobowiązania o zachowaniu poufności.