Zarządzenie Nr .7.../2009
Starosty Rybnickiego
z dnia 12 marca 2009 r.

W sprawie wprowadzenia instrukcji służących ochronie danych osobowych zgromadzonych w rejestrach prowadzonych przez Referat Komunikacji w Starostwie Powiatowym w Rybniku

Na podstawie art. 36 ust. 1 w związku z art. 7 pkt 4 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (j.t. Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz art.35 ust. 2 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (j.t. Dz.U. z 2001 r. Nr 142, poz. 1592 z późn. zm.)

zarządzam co następuje:

§ 1

Wprowadzam:

1) instrukcję określającą sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych Pojazd i Kierowca w Starostwie Powiatowym w Rybniku w brzmieniu określonym w załączniku Nr 1 do niniejszego zarządzenia;
2) instrukcję postępowania awaryjnego w przypadku zalania pomieszczeń w brzmieniu określonym w załączniku Nr 2 do niniejszego zarządzenia.

§2

Wykonanie zarządzenia powierzam Sekretarzowi Powiatu i koordynatorowi w Referacie Komunikacji.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA
mgr Damian Mrowiec

Załącznik Nr 1

INSTRUKCJA

określająca sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych Pojazd i Kierowca w Starostwie Powiatowym w Rybniku

§ 1

1. Instrukcja określa sposób zarządzania lokalnym systemem informatycznym Pojazd i Kierowca w zakresie przetwarzania danych osobowych i realizuje wymagania, o którym mowa w par. 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 niniejszą instrukcją należy stosować postanowienia Instrukcji Bezpieczeństwa Systemu Pojazd i Kierowca w Urzędzie oraz Zarządzenia Nr 3/07 Starosty Rybnickiego z dnia 15 marca 2007 r. w sprawie zasad bezpieczeństwa informatycznego w Starostwie Powiatowym w Rybniku.

3. Przez użyte w instrukcji określenia należy rozumieć :
   1) UODO – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;
   2) ADO - Administrator Danych Osobowych – Starosta (organ ,o którym mowa w art.3 UODO, który decyduje o celach i środkach przetwarzania danych osobowych)
   3) ABI - Administrator Bezpieczeństwa Informacji – osoba, która nadzoruje przestrzeganie zasad ochrony danych osobowych, powołana przez ADO chyba, że ADO sam wykonuje te czynności ; / art. 36 ust.3 UODO /
   4) RMSWiA – Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., o którym mowa w ust. 1 ;
   5) PBSPiK – Polityka Bezpieczeństwa Systemów Pojazd i Kierowca;
   6) IBSPiK – Instrukcja Bezpieczeństwa Systemu Pojazd w Urzędzie i Instrukcja Bezpieczeństwa Systemu Kierowca w Urzędzie

§ 2

1. System informatyczny , w którym są przetwarzane dane osobowe musi spełniać wymagania określone w RMSWiA i PBSPiK;

2. W szczególności system zapewnia dla każdej osoby, której dane osobowe są w nim przetwarzane automatycznie odnotowanie :
   1) daty pierwszego wprowadzania 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 i kiedy zostały udostępnione dane, w rozumieniu art.7 pkt 6 UODO ;

3. System winien pracować w produkcyjnej , dedykowanej sieci teleinformatycznej.
4. Przez sieć produkcyjną , o której mowa w ust. 3 rozumie się sieć odseperowaną, tj. bezpośredniego lub pośredniego połączenia z internetem i z ograniczonym, zarządzalnym połączeniem z innymi sieciami produkcyjnymi.
5. Dane osobowe mogą być przetwarzane na komputerach przenośnych tylko jeżeli systemy plików na dyskach twardych są szyfrowane, a dostęp do klucza kryptograficznego jest autoryzowany za pomocą hasła, tokenu lub certyfikatu elektronicznego.
6. Pliki zawierające dane osobowe przesyłane przez łącza publiczne muszą być szyfrowane.
7. System uniemożliwia użytkownikom dostęp do ustawień BIOS.
8. Korzystanie z nośników wymiennych podlega ograniczeniom i podlega autoryzacji.
9. Pomieszczenia, w których eksploatowany jest system są chronione przed dostępem osób nieuprawnionych.

§ 3

1. Dostęp do pomieszczeń i systemu, w którym przetwarzane są dane osobowe jest przyznawany osobom upoważnionym do przetwarzania danych osobowych (załącznik nr 1), które formalnie zobowiązały się do :
   1) zachowania w tajemnicy przetwarzanych danych osobowych oraz informacji dotyczących środków ich przetwarzania;
   2) niewykraczania poza uprawnienia przyznane w systemie.
2. Tworzenia konta, zmiana lub zawieszenie praw dostępu w systemie dla użytkowników są realizowane przez Polską Wytwórnię Papierów Wartościowych S.A. Zgodnie z procedurami określonymi w IBSPiK na formalny wniosek osoby upoważnionej przez Starostę Rybnickiego.

§ 4

1. W systemie stosuje się uwierzytelniania z użyciem imiennego certyfikatu x509v3 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. W systemie stosuje się hasła o poziomie złożoności określonym w zabezpieczeniu nr VIII załącznika do RMSWiA.
6. Systemy nie zezwalają na ustanowienie :
   1) hasła krótszego niż 8 znaków;
   2) kodu PIN do karty o długości krótszej niż 4 znaki;
7. Systemy uniemożliwiają uwierzytelnienie użytkownika przez 30 minut jeśli trzy kolejne próby uwierzytelniania zakończyły się niepowodzeniem.
8. Hasło i kod PIN są informacjami przeznaczonymi wyłącznie do wiadomości użytkownika systemu i nie powinny być ujawniane osobom trzecim.
9. Dopuszcza się poniższe wyjątki od zasady przytoczonej w ust. 8:
   1) awaryjne hasło użytkownika systemów Kierowca i Pojazd jest czasowo przechowywane w PWPW S.A., gdzie generowane są listy haseł logowania awaryjnego;

   2) tymczasowy kod PIN karty użytkownika może być znany administratorowi systemu

w PWPW S.A bezpośrednio po odblokowaniu karty na wniosek użytkownika;

10. W celu złagodzenia ryzyk wynikających z wyjątków wymienionych w ust. 9 :
    1) użytkownik systemu powinien zmienić kod PIN niezwłocznie po jego ustanowieniu przez administratora;
    2) kopia listy haseł logowania awaryjnego przechowywana w PWPW jest niszczona niezwłocznie po uzyskaniu potwierdzenia dostarczenia jej oryginału do starostwa.
11. Hasła i kody PIN w stosunku do których zaistniało podejrzenie ich ujawnienia podlegają niezwłocznej zmianie zgodnie z zasadami określonymi w IBSPiK .

§ 5

1. Rozpoczynając pracę w systemie użytkownik uwierzytelnia się w systemie operacyjnym. Wprowadzanie hasła lub kodu PIN musi odbywać się w sposób uniemożliwiający ich ujawnienie innym osobom.
2. W przypadku braku możliwości rozpoczęcia pracy lub powzięcia podejrzeń, że z konta użytkownika mogła korzystać inna osoba bądź jakiegokolwiek innego naruszenia bezpieczeństwa systemu należy niezwłocznie powiadomić operatora infolinii (telefon 0801-300-403) lub bezpośrednio zespół bezpieczeństwa w PWPW S.A. (telefon 0225302334).
3. Ustawienie monitora lub zastosowanie filtra ograniczającego kąt widzenia powinno uniemożliwić podgląd ekranu osobom nieupoważnionym do przetwarzania danych osobowych.
4. W przypadku konieczności opuszczenia stanowiska pracy, użytkownik systemu obowiązany jest uniemożliwić dostęp do stacji roboczej aktywując wygaszacz ekranowy zabezpieczony hasłem
5. Zabezpieczenie, o którym mowa w ust. 4 powinno być aktywowane automatycznie jeśli stacja robocza nie była wykorzystywana przez 20 minut.
6. Po zakończeniu pracy przy przetwarzaniu danych osobowych użytkownik powinien wylogować się z systemu i wyłączyć komputer.

§ 6

1. Wykonywanie, przechowywanie i likwidacja kopii bezpieczeństwa powinny być realizowane zgodnie z zasadami określonymi w IBSiK.
2. PWPW S.A. odpowiada za inicjowanie, wykonywanie i weryfikację poprawności zapisu na nośnikach.
3. Wyznaczony pracownik starostwa odpowiada za jednoznaczne oznaczenie nośników, ich wymianę w napędzie zgodnie z ustalonym harmonogramem oraz za przechowywanie nośników w miejscu oddalonym od miejsca, w którym zlokalizowany jest serwer i w sposób uniemożliwiający nieuprawnione przejęcie, odczyt, modyfikację, uszkodzenie lub zniszczenie.
4. Za niszczenie nośników po ich wycofaniu z użycia odpowiada Starostwo.

§ 7

1. Elektroniczne nośniki informacji 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, modyfikację, uszkodzenie lub zniszczenie.
3. Wprowadzenie i wycofanie z użycia i niszczenie elektronicznych nośników informacji powinno się odbywać zgodnie z :
    1) PBSPiK w przypadku dysków twardych zainstalowanych w serwerach i stacjach

roboczych;
2) w oparciu o Zarządzenie Nr 3/07 Starosty Powiatu Rybnickiego w dnia 15 marca 2007 r. w przypadku nośników wymiennych.

4. Nośniki elektroniczne powinny być pozbawiane zapisanych na nich danych lub fizycznie niszczone niezwłocznie po ustaniu celu w jakim dane zostały na nich zapisane.
5. Nieuzasadnione kopiowanie danych osobowych na nośniki jest zabronione.

§ 8

1. Ochrona przed szkodliwym oprogramowaniem jest realizowana przez oprogramowanie antywirusowe instalowane na serwerach i stacjach roboczych.
2. Oprogramowanie antywirusowe i bazy sygnatur szkodliwego oprogramowania są aktualizowane przez PWPW S.A zgodnie ze szczególnymi wymaganiami określonymi PBSiK.

§ 9

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 Starostwa.
3. Jeżeli wykonanie czynności serwisowych wymaga dostępu do danych osobowych to pracownik firmy zewnętrznej jest zobowiązany do podpisania zobowiązania o zachowaniu poufałości.
4. Urządzenia komputerowe, dyski twarde lub inne elektroniczne nośniki danych,przeznaczone do naprawy, pozbawia się przed naprawą zapisu danych osobowych lub naprawia się je pod nadzorem pracownika Starostwa.

ZATWIERDZIŁ:

STAROSTA

mgr Damian Mrowiec

.....

Załącznik Nr 2

Instrukcja Postępowania Awaryjnego w przypadku zalania pomieszczeń

W STAROSTWIE POWIATOWYM W RYBNIKU - WYDZIAŁ KOMUNIKACJI

CEL OPRACOWANIA

Opracowanie instrukcji służy do zabezpieczeń danych w przypadku zalania lub zatopienia pomieszczeń w których są przetwarzane dane osobowe zgodnie z ustawą, z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.(Dz. U. z dnia 29 października 1997 r.)

ZABEZPIECZENIE

Rurociągi wody pitnej, kanalizacyjne przechodzące przez pokoje archiwum gdzie znajdują się lub przetwarzane są dane osobowe powinny być zabezpieczone przed grawitacyjnym opadem ścieków lub czystej wody .
W miejscach gdzie znajdują się rurociągi powyżej regałów lub przetwarzania danych należy wykonać stałe osłony zabezpieczające przed bezpośrednim zalaniem akt osobowych.W miejscach przechowywania danych osobowych powinien znajdować się monitoring zgodnie z patentem Nr P - 368696) Zalanie z powodu awarii instalacji wodnej, niedokręconych zaworów, pękniętych rur kanalizacyjnych zdarza się to często i powoduje duże straty materialne. System Suchy Dom ® działa po wykryciu najmniejszego wycieku, sygnalizując jego powstanie lub odcinając dopływ, co daje możliwość natychmiastowej interwencji: W razie wykrycia obecności wody system odcina dopływ wody na rurze zasilającej i/lub uruchamia odpowiednią sygnalizację: akustyczną, optyczną, do nadajnika monitoringu lub do automatyk .Czujniki umieszczone w wybranych miejscach wykrywają nawet minimalną ilość wody (ok. 1 mm) na powierzchni np. podłogi lub zmianę poziomu w zbiorniku .Przerwy w zasilaniu sieci elektrycznej lub jakiekolwiek zakłócenia postronne nie wpływają na skuteczność systemu .

POSTĘPOWANIE W RAZIE BRAKU MONITORINGU STAŁEGO

W czasie braku systemu monitoringu stałej kontroli pomieszczeń przechowywania danych oraz przetwarzania danych należy kontrolować korytarz Wydziału Komunikacji celem sprawdzenia czy na korytarzu znajduje się woda.

Kontrola korytarza Wydziału Komunikacji powinna odbyć się nie rzadziej niż co 2 godziny

Progi pomiędzy archiwum a korytarzem SA w wysokości około 3 cm .

Regały na których znajdują się dokumenty Wydziału Komunikacji są na wysokości 8 cm . obniżone pokoje tworzą misę dlatego należy kontrolować korytarz celem identyfikacji zagrożeń przed zalaniem .

Kierownik Wydziału Komunikacji wyznaczy osobę imiennie i stanowiskiem uprawnioną do otwarcia archiwum w razie wystąpienia awarii zalania wodą .

W razie absencji z powodu urlopu lub chorobowego należy wyznaczyć następna uprawniona osobę w razie awarii.

Każdorazowe wejście należy wpisać do dziennika ochrony znajdującej się w portierni .

Dokumentacja wejść awaryjnych powinna być również odnotowana w Wydziale k Komunikacji.

Każdorazowe wejście powinno być potwierdzone podpisem osoby upoważnionej z dokładna data , godziną i minutą .

RODZAJ ZAGROŻENIA

Podstawowym zagrożeniem zalania lub zatopienia dokumentów jest utracenie danych osobowych lub dokumentów związanych z rejestracja pojazdów .

POŻAR

Małe pożary należy gasić gaśnicami proszkowymi na wyposażeniu Wydziału Komunikacji .
Gaszenie gaśnicami proszkowymi przeznaczone do gaszenie zgodnie z klasyfikacji A – materiały stałe .
W czasie pożaru należy unikać otwieranie okien , przewietrzania pomieszczeń w czasie spalania .
W pomieszczeniach gdzie znajdują się dane osobowe należy unikać gaszenie pożaru gaśnicami pianowymi oraz wodą .

Opracował

INSPEKTOR PPOŻ
Ryszard Michalski

Zatwierdził

STAROSTA
mgr Damian Mrowiec