Załącznik nr 2
do Zarządzenia nr 7/2013
Przewodniczącego Zarządu Związku Gmin Krajny w Złotowie
z dnia 21sierpnia 2013r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Związku Gmin Krajny w Złotowie

§1.Niniejsza instrukcja określa szczegółowe zasady zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych Związku Gmin Krajny w Złotowie.

1. Procedura nadawania i odbierania uprawnień do przetwarzania danych osobowych:
2. Konto użytkownika na serwerze zakłada administrator serwera, na podstawie upoważnienia do przetwarzania danych osobowych. Rejestracja w systemie polega na nadaniu identyfikatora i przydziale hasła oraz wprowadzeniu tych danych do bazy użytkowników domeny Active Directory
3. Dla użytkowników nie logujących się do systemu Qnet tworzy się konto z ograniczonymi prawami na stacji roboczej Windows.
4. W identyfikatorze pomija się polskie znaki diakrytyczne.
5. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika administrator systemu, za zgodą administratora bezpieczeństwa informacji, nadaje inny identyfikator odstępując od zasady określonej w ppkt. 2).
6. Administrator systemu nadaje uprawnienia użytkownikom do poszczególnych funkcji programu zgodnie z zakresem upoważnienia.
7. Wyrejestrowania użytkownika z systemu informatycznego dokonuje administrator systemu na wniosek pracownika ds. kadrowo – płacowych.
8. Wyrejestrowanie, o którym mowa powyżej, może mieć charakter czasowy lub trwały.
9. Wyrejestrowanie następuje poprzez:
   1) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
   2) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).
10. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego jest: zawieszenie w pełnieniu obowiązków służbowych, zwolnienie z pełnienia obowiązków służbowych.
11. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy użytkownika. Nazwa użytkownika nie może być przydzielona innej osobie.

Stwierdzam prawdziwość niniejszej Instrukcji pod względem formalnoprawnym. Kopia strona została podpisana.

RADCA PRAWNY
Radosław Kilar

12. Administrator serwera jest użytkownikiem uprzywilejowanym, posiadającym najwyższe uprawnienia w systemie informatycznym.
    1) Konto użytkownika uprzywilejowanego jest używane tylko w uzasadnionych przypadkach.
    2) Hasło administratora serwera jest przechowywane w szafie pancernej w pomieszczeniu administratora serwera.

§2. Metody i środki uwierzytelniania:

1. Uwierzytelnianie użytkownika w systemie informatycznym następuje po podaniu nazwy użytkownika i hasła.
2. Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
    1) Hasło nie może być identyczne z identyfikatorem użytkownika, ani z jego imieniem lub nazwiskiem.
    2) Hasło nie może być zapisane w miejscu dostępnym dla osób nieuprawnionym.
    3) Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom.
3. Procedury rozpoczęcia, zwieszenia i zakończenia pracy w systemie informatycznym:
4. Rozpoczęcie pracy w systemie odbywa się poprzez:
    1) przygotowanie stanowiska pracy,
    2) włączenie stacji roboczej,
    3) wprowadzenie swojego identyfikatora i hasła w domenie Active Directory
6. Zawieszenie pracy w przypadku czasowego opuszczenia stanowiska pracy:
    1) zablokowanie ekranu na komputerze przy użyciu klawiszy Windows + L,
    2) odblokowanie ekranu po padaniu hasła,
7. Zakończenie pracy w systemie odbywa się poprzez:
    1) zamknięcie aplikacji,
    2) odłączenie się od zasobów systemowych,
    3) zamknięcie systemu operacyjnego,
    4) wyłączenie stacji roboczej.

§3.1. Zabrania się użytkownikom pracującym w systemie:

1) udostępniania stacji roboczej osobom nie zarejestrowanym w systemie,
2) udostępniania stacji roboczej do konserwacji lub naprawy bez porozumienia z administratorem bezpieczeństwa informacji,
3) logowania się na lokalne konto stacji roboczej
4) używania nie licencjonowanego oprogramowania.
5) instalacji oprogramowania bez zgody administratora sieci

2. Każdy przypadek naruszenia ochrony danych osobowych, a w szczególności:

EGZEMPLARZ SŁUŻBOWY
EGP - 209
Radosław Kilar

1) naruszenia bezpieczeństwa systemu informatycznego,
2) stwierdzenia objawów (stanu urządzeń, sposobu działania programu lub jakości komunikacji w sieci), które mogą wskazywać na naruszenie bezpieczeństwa

3. podlega zgłoszeniu do administratora bezpieczeństwa informacji i .administratorowi sieci informacji zgłasza się w szczególności przypadki:
   1) użytkowania stacji roboczej przez osobę nie będącą użytkownikiem systemu,
   2) usiłowania logowania się do systemu (sieci) przez osobę nieuprawnioną,
   3) usuwania, dodawania lub modyfikowania bez wiedzy i zgody użytkownika jego dokumentów (rekordów),
   4) przebywania osób nieuprawnionych w obszarze, w którym przetwarzane są dane osobowe,

      w trakcie nieobecności osoby zatrudnionej przy przetwarzaniu tych danych i bez zgody administratora danych, pozostawiania bez nadzoru otwartych pomieszczeń, w których przetwarzane są dane osobowe,
   5) udostępniania osobom nieuprawnionym stacji roboczej lub komputera przenośnego, służących do przetwarzania danych osobowych,
   6) nie zabezpieczenia hasłem dostępu do komputera służącego do przetwarzania danych osobowych,
   7) przechowywania kopii awaryjnych w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco,
   8) przechowywania nośników informacji oraz wydruków z danymi osobowymi, nie przeznaczonymi do udostępniania, w warunkach umożliwiających do nich dostęp osobom nieuprawnionym.
4. Obowiązek dokonania zgłoszenia, o którym mowa w pkt 3, spoczywa na każdym pracowniku, który powziął wiadomość o naruszeniu ochrony danych osobowych.

§4.1. W przypadku naruszenia integralności bezpieczeństwa sieciowego, obowiązkiem administratora jest natychmiastowe wstrzymanie udostępniania zasobów dla użytkowników i odłączenie serwerów od sieci.

2. Administrator sieci w porozumieniu z administratorem bezpieczeństwa informacji ustalają przyczyny naruszenia integralności bezpieczeństwa sieciowego.
3. Przywrócenie udostępniania zasobów użytkownikom może nastąpić dopiero po ustaleniu i usunięciu przyczyny naruszenia integralności bezpieczeństwa sieciowego.

§5 Procedura tworzenia kopii zapasowych.

1. Nośniki zawierające kopie zapasowe są odpowiednio oznaczone i przechowywane w szafie pancernej administratora systemu.
2. Zabrania się przechowywania kopii awaryjnych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu.

RADCA PRAWNY RADCA PRAWNY
BdP - 209
Radosław Kilar

3. Administrator systemu przegląda okresowo kopie awaryjne i ocenia ich przydatność do odtworzenia zasobów systemu w przypadku jego awarii.
4. Stwierdzenie utraty przez kopie awaryjne waloru przydatności do celu, o którym mowa w ust. 3, upoważnia administratora systemu do ich zniszczenia.
5. Nośniki danych przeznaczone do likwidacji są niszczone w sposób uniemożliwiający odczyt danych.

§6 Procedura zabezpieczenia systemu informatycznego.

1. Sprawdzanie obecności wirusów komputerowych w systemie oraz ich usuwanie odbywa się przy wykorzystaniu licencjonowanego oprogramowania w oparciu o serwer dystrybucji aktualnych sygnatur i wersji oprogramowania.
2. Administrator systemu nie rzadziej niż raz na tydzień przeprowadza pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach, jak również w serwerach i stacjach roboczych.
3. Do obowiązków administratora systemu należy aktualizacja oprogramowania służącego do sprawdzania w systemie obecności wirusów komputerowych.
4. System i urządzenia informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, zabezpiecza się przed utratą danych osobowych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej,
5. Minimalne zabezpieczenie systemu i urządzeń informatycznych polega na wyposażeniu serwera (serwerów) oraz stacji roboczych w zasilacze awaryjne (UPS).
6. W systemach działających sieciowo, na zasadzie udostępnienia zasobów na serwerze, administrator systemu powinien uwzględniać dedykowane przyzwolenia dostępu.
7. Przesyłanie danych osobowych w komunikacji wewnętrznej (LAN) musi być oznaczone w sposób dostępny jedynie dla uprawnionych użytkowników i wyznaczony przez administratora sieci, przy użyciu narzędzi zabezpieczeń w obrębie systemu informatycznego.

§6.1. W sytuacji, gdy dostępne narzędzia informatyczne nie będą wystarczające do działania w komunikacji wewnętrznej, administrator sieci wyznacza sposób postępowania, mając w szczególności na uwadze ochronę danych osobowych.

2. Do przesyłania danych przy połączeniach w sieci publicznej (Internet), z uwagi na przekazywane dane osobowe, powinny być wykorzystywane tylko kanały transmisji wykorzystywane przez autoryzowane programy wykorzystywane również w innych urzędach oraz Instytucjach Państwowych i przepisy prawne uwzględniające wysyłanie tych danych.

§7.1. Nośniki informatyczne zawierające dane osobowe powinny być opisane w sposób czytelny i zrozumiały dla użytkownika, a zarazem nie powinny ułatwiać rozpoznania zawartości przez osoby nieupoważnione.

2. Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione.

RADCA PRAWNY
EDP - 209
Radosław Kilar

3. Osoby użytkujące przenośne nośniki informatyczne, służące do przetwarzania danych osobowych, obowiązane są niezwłocznie informować na piśmie administratora bezpieczeństwa informacji o zakresie, rodzaju zbieranych danych osobowych oraz celu ich przetwarzania. Administrator bezpieczeństwa informacji może żądać usunięcia danych, co do których zachodzi uzasadnione podejrzenie, że nie są przetwarzane zgodnie z zasadami określonymi w przepisach o ochronie danych osobowych.
4. Osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem ochrony danych w celu zapobieżenia dostępowi do tych danych osobie niepowołanej.

§8.1. Użytkownik sporządzający wydruki, które zawierają dane osobowe jest odpowiedzialny za zachowanie szczególnej ostrożności przy korzystaniu z nich, a zwłaszcza za zabezpieczenie ich przed dostępem osób nie posiadających imiennego upoważnienia oraz nieuprawnionych do wglądu na podstawie indywidualnego zakresu czynności.

2. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.
3. System powinien umożliwić udostępnienie na piśmie, w zrozumiałej formie, treści danych o każdej osobie, której dane są przetwarzane, a w szczególności:
   1) daty pierwszego wprowadzenia danych tej osoby,
   2) źródła pochodzenia danych,
   3) nazwy użytkownika wprowadzającego dane,
   4) informacji - komu, kiedy i w jakim zakresie dane zostały udostępnione,
   5) sprzeciwu, o którym mowa w art. 32 ust. l pkt. 7, po jego uwzględnieniu, oraz sprzeciwu określonego w art. 32 ust. 1 pkt. 8 ustawy o ochronie danych osobowych.

§9 Konserwacja systemu informatycznego.

1. Administrator serwera codziennie sprawdza logi systemowe i programowe.
2. Administrator serwera okresowo sprawdza spójność danych oraz stan nośników (dysków twardych).
3. Przeglądu i konserwacji systemu dokonuje administrator systemu doraźnie.
4. Przeglądu pliku zawierającego raport dotyczący działalności aplikacji bądź systemu (log systemowy) administrator systemu dokonuje nie rzadziej niż raz na tydzień.
5. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje administrator systemu nie rzadziej niż raz na tydzień.

§10. Naprawa i likwidacja urządzeń informatycznych.

1. urządzenia informatyczne służące do przetwarzania danych osobowych można przekazać: do naprawy, podmiotowi nieuprawnionemu do otrzymania tych danych, do likwidacji dopiero po uprzednim uzyskaniu zgody administratora bezpieczeństwa informacji.

RADCA PRAWNY
ŁDP - 209
Radosław Kilar

2. Urządzenia, o których mowa w pkt l, przed ich przekazaniem pozbawia się zapisu danych osobowych.
3. Jeżeli nie jest to możliwe, urządzenie to może być naprawiane wyłącznie pod nadzorem osoby pisemnie upoważnionej przez administratora bezpieczeństwa informacji.
4. Jeżeli nie jest możliwe pozbawienie urządzenia przekazywanego do likwidacji zapisu danych osobowych, urządzenie - przed przekazaniem - uszkadza się w sposób uniemożliwiający odczytanie tych danych.