WÓJT GMINY ELBLĄG
ul. Browarna 85
82-300 ELBLĄG

Zarządzenie Nr ..41...../2009 r.
Wójta Gminy Elbląg
z dnia 30. września 2009 r.

w sprawie: w sprawie wydania instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Elbląg

Na podstawie §3 ust. 2 i 3 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie 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

Z dniem 01 października 2009 roku wprowadzam jako obowiązującą w Urzędzie Gminy Elbląg, Instrukcję określającą sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Elbląg, stanowiącą załącznik do niniejszego Zarządzenia.

§ 2

Zobowiązuje wszystkich pracowników zatrudnionych na stanowiskach pracy z dostępem, przetwarzaniem i wykorzystywaniem danych osobowych do bezwzględnego przestrzegania postanowień Instrukcji .

§ 3

Wydana Instrukcja podlega przepisom ochrony tajemnicy państwowej i służbowej na zasadzie art. 100 § 2 pkt 4 Kodeksu pracy

§ 4

Zarządzenie wchodzi w życie z dniem 01.10.2009 r.

WÓJT
mgr inż. Genowefa Kwoczek

Załącznik do Zarządzenia
Wójta Gminy Elbląg Nr 41/2008
Z dnia 30 września 2008r.

Instrukcja określająca sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Elbląg

§ 1 Instrukcja określa sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

§ 2 Zakres zastosowania

Instrukcja określa zasady zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, a w szczególności: sposób rejestrowania i wyrejestrowania użytkownika, sposób przydziału haseł i zasady korzystania z nich, procedury rozpoczęcia i zakończenie pracy, obowiązki użytkownika, metodę i częstotliwość tworzenia kopii, zasady sprawdzania obecności wirusów komputerowych oraz dokonywania przeglądów i konserwacji systemu.

§ 3 Obszar przetwarzania danych:

1. Obszar przetwarzania danych osobowych z użyciem sprzętu komputerowego stanowi obszar budynku przy ul. Browarnej 85 w Elblągu.
2. Wszystkie pomieszczenia, które należą do obszaru przetwarzania danych, wyposażone są w zamknięcia. W czasie, gdy nie znajdują się w nich osoby upoważnione, pomieszczenia są zamykane w sposób uniemożliwiający wstęp osobom nieupoważnionym.

§4 Rejestrowania i wyrejestrowania użytkownika

1. Użytkownikiem systemu informatycznego (osobą upoważnioną) może być:
   a. osoba zatrudniona przy przetwarzaniu danych osobowych w Urzędzie Gminy Elbląg, która posiada upoważnienie do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład,
   b. pracownik innego podmiotu lub przedsiębiorca będący osobą fizyczną prowadzi działalność na podstawie wpisu do ewidencji działalności gospodarczej, którzy świadczą na podstawie stosowanych umów usługi związane z ich pracą w systemie informatycznym (serwis, zlecenie przetwarzania danych osobowych itp.).
2. Uzyskanie uprawnień następuje na dwóch poziomach:
   a. zarejestrowania w sieci komputerowej (złożenie konta),
   b. nadanie określonych uprawnień do systemów aplikacyjnych.

3. Pisemny wniosek o zarejestrowanie użytkownika składa bezpośredni przełożony pracownika. Wniosek zostaje przekazany do Sekretarza/Administratora sieci/Administratora Bezpieczeństwa Informacji, który może zgłosić sprzeciw wobec przyznania uprawnień, ze względu na zagrożenie naruszenia bezpieczeństwa danych osobowych.
4. Jednocześnie z wnioskiem o zarejestrowanie użytkownika, przełożony składa pisemny wniosek do administratora systemu o nadanie określonych uprawnień do systemów aplikacyjnych.
5. Postanowienie §4 pkt. 4 stosuje się odpowiednio w przypadku przejścia pracownika do innej komórki organizacyjnej. Obowiązek złożenia wniosku o nadanie uprawnień spoczywa na nowym bezpośrednim przełożonym pracownika.
6. W przypadku zakończenia pracy w Urzędzie Gminy Elbląg, stosuje się następująca procedurę wyrejestrowania użytkownika:
   a. na karcie obiegowej, na której osoba odchodząca zbiera podpisy potwierdzenia rozliczenia się z pracodawcą, znajduje się pozycja stwierdzająca fakt usunięcia lub zablokowania profilu użytkownika,
   b. Sekretarz przed podpisaniem pozycji stwierdzającej fakt usunięcia lub zablokowania profilu użytkownika wydaje polecenie administratorowi systemu o natychmiastowym wykonaniu tej czynności,
   c. po wykonaniu tej czynności następuje podpisanie przez Sekretarza obiegówki potwierdzającej usunięcie lub zablokowanie profilu użytkownika,
   d. wykonanie tej operacji jest jednoznaczne z uniemożliwieniem dostępu do systemu dla pracownika, z którym rozwiązano umowę o pracę w Urzędzie Gminy Elbląg,
   e. Sekretarz zawiadamia Administratora Bezpieczeństwa Informacji o fakcie wyrejestrowania użytkownika.

§ 4 Sposób przydziału haseł i zasady korzystania z nich

1. Każdorazowe uwierzytelnienie użytkownika w systemie następuje po podaniu identyfikatora i hasła.
2. Używanie hasła jest obowiązkowe dla każdego użytkownika, posiadającego identyfikator.
3. W Urzędzie Gminy Elbląg obowiązują następujące zasady korzystania z haseł:
   a. zabrania się ujawniania haseł jakimkolwiek osobom trzecim,
   b. zabrania się zapisywania haseł lub takiego z nimi postępowania, które umożliwia lub ułatwia dostęp do haseł osobom trzecim.
4. Prawidłowe wykonywanie obowiązków związanych z korzystaniem użytkowników z haseł

nadzoruje Administrator Bezpieczeństwa Informacji.

§ 5 Rozpoczęcie i zakończenie pracy

1. Przed przystąpieniem do pracy w systemie informatycznym użytkownik zobowiązany jest sprawdzić urządzenie komputerowe i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych. W przypadku naruszenia ochrony danych osobowych użytkownik niezwłocznie powiadamia Administratora Bezpieczeństwa Informacji.
2. Użytkownik rozpoczyna pracę w systemie informatycznym od następujących czynności:
   a. włączenia komputera,
   b. uwierzytelnienia się („zalogowania" w systemie) za pomocą identyfikatora i hasła.
3. Niedopuszczalne jest uwierzytelnianie się na hasło i identyfikator innego użytkownika lub praca w systemie informatycznym na koncie innego użytkownika.
4. Zakończenie pracy użytkownika w systemie następuje po „wylogowaniu się" z systemu. Po zakończeniu pracy użytkownik zabezpiecza swoje stanowisko pracy, w szczególności dyskietki, dokumenty i wydruki zawierające dane osobowe, przed dostępem osób nieupoważnionych.
5. W przypadku dłuższego opuszczenia stanowiska pracy, użytkownik zobowiązany jest „wylogować się" lub zaktywizować wygaszacz ekranu z opcją ponownego „logowania" się do systemu.
6. W przypadku wystąpienia nieprawidłowości w mechanizmie uwierzytelniania („logowaniu się" w systemie), użytkownik niezwłocznie powiadamia o nich administratora.

§ 6 Tworzenie, przechowywanie, sprawdzanie przydatności i likwidacji kopii zapasowych.

1. Kopie zapasowe są tworzone, przechowywane i wykorzystywane z uwzględnieniem następujących zasad:
   a. kopie wykonywane są codziennie,
   b. kopie wykonywane są na nośnikach wg. schematu rotacji tygodniowej – tzn na jednym nośniku zapisany jest stan z jednego dnia tygodnia,
   c. kopie są okresowo, raz w miesiącu, sprawdzane pod kątem ich przydatności do odtworzenia danych, a jeżeli ustanie ich użyteczność są niezwłocznie usuwane.

§ 7 Sprawdzanie obecności wirusów komputerowych:

1. Sprawdzanie obecności wirusów komputerowych dokonywane jest poprzez zainstalowanie programu, który skanuje automatycznie, bez udziału użytkownika, na obecność wirusów wszystkie pliki. Program jest zainstalowany na wszystkich serwerach i stacjach

roboczych.

2. Po każdej naprawie i konserwacji komputera należy dokonać sprawdzenia pod kątem występowania wirusów i ponownie zainstalować program antywirusowy.

§ 8 Sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków:

1. Wydruki i dokumenty papierowe zawierające dane osobowe przechowywane są wyłącznie w odrębnych zamykanych szafach.
2. Osoba zatrudniona przy przetwarzaniu danych osobowych sporządzająca wydruk zawierający dane osobowe ma obowiązek na bieżąco sprawdzać przydatność wydruku w wykonywanej pracy, a w przypadku jego nieprzydatności – niezwłocznie wydruk skutecznie zniszczyć.
3. Elektroniczne nośniki informacji z danymi osobowymi są oznaczane i przechowywane w zamykanych szafach lub.
4. Fizyczna likwidacja zniszczonych lub niepotrzebnych elektronicznych nośników informacji z danymi osobowymi odbywa się w sposób uniemożliwiający odczyt danych osobowych.
5. Dopuszczalne jest zlecenie/powierzenie niszczenia wszelkich nośników danych osobowych wyspecjalizowanym podmiotom zewnętrznym. Podstawą przekazania danych do zniszczenia innemu podmiotowi powinna być w każdym przypadku umowa zawarta na piśmie.

§ 9 Zasady przeglądów i konserwacji systemu:

1. Przegląd i konserwacja zbiorów danych dokonywane są poprzez:
   a. badanie spójności bazy danych,
   b. uruchamianie zapytań do bazy danych w celu analizy danych,
   c. przegląd wydruków po wyznaczonych procesach,
   d. sprawdzanie zgodności danych z dokumentami,
   e. analiza zgłaszanych uwag użytkowników.
2. Przeglądu i konserwacji dokonują informatyk, w porozumieniu z Administratorem Bezpieczeństwa Informacji.
3. W przypadku zlecenia wykonywania czynności, o których mowa wyżej, podmiotowi zewnętrznemu, wszelkie prace powinny odbywać się pod nadzorem Administratora Bezpieczeństwa Informacji.

§ 10 Komunikacja w sieci komputerowej:

1. W zakresie korzystania z sieci komputerowej w Urzędzie Gminy Elbląg obowiązują

następujące zasady:

a. pracownicy nie są uprawnieni do instalacji jakiegokolwiek prywatnego oprogramowania bez odpowiedniej zgody Wójta Gminy Elbląg. W przypadku zainstalowania takiego oprogramowania bez odpowiedniej akceptacji pracownik ponosi odpowiedzialność porządkową i prawną,
b. oprogramowanie na komputerach może być zainstalowane wyłącznie przez informatyka,
c. wszelkie dane zainstalowane na komputerach Urzędu stanowią własność Gminy,
d. pracownicy mogą używać połączenia z Internetem jedynie w celach służbowych,
e. pracownicy nie mają prawa przekazywać za pośrednictwem sieci komputerowej do stron trzecich jakichkolwiek danych stanowiących własność Gminy,
f. pracownicy nie mogą ściągać za pośrednictwem sieci komputerowej żadnego oprogramowania,
g. pracownicy nie mogą podłączać się do sieci zewnętrznej za pośrednictwem modemów.

§ 11 Obowiązki i odpowiedzialność użytkownika związane obowiązywaniem instrukcji

1. Użytkownik systemu jest zobowiązany zapoznać się z treścią niniejszej Instrukcji i potwierdzić to stosownym oświadczeniem.
2. Naruszenie przez pracownika niniejszej Instrukcji może zostać potraktowane jako naruszenie obowiązków pracowniczych i powodować określoną przepisami Kodeksu pracy odpowiedzialność pracownika.

WÓJT

mgr inż. Genowefa Kwoczek