Załącznik nr 1
do Polityki Bezpieczeństwa Informacji
z dnia 30 sierpnia 2012 roku.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

I
Postanowienia ogólne

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „Instrukcją", określa procedury dotyczące zasad bezpieczeństwa przetwarzania danych osobowych oraz zasady postępowania administratora danych osobowych, osób przez niego wyznaczonych i użytkowników przetwarzających dane osobowe w **Urząd Gminy Secemin**
2. W systemach informatycznych służących do przetwarzania danych osobowych stosuje się środki bezpieczeństwa na poziomie wysokim.

II
Rejestrowanie w systemie informatycznym

1. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, mogą zostać dopuszczone, wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych, wydane przez administratora danych osobowych.
2. Przyznanie uprawnień do przetwarzania danych osobowych w systemie informatycznym polega wypełnieniu karty uprawnień przez Kierownika Referatu według wzoru - Załącznik nr 1 do Instrukcji Zarządzania Systemem Informatycznym, następnie po akceptacji przez Administratora Bezpieczeństwa Informacji dokument jest przekazywany Administratorowi Systemów Informatycznych (ASI).
3. Administratorowi Systemów Informatycznych zakłada identyfikator sieciowy/konto w systemach informatycznych i przekazuje login i hasło tymczasowe użytkownikowi. Użytkownik przy

pierwszym logowaniu zobowiązany jest zmienić hasło na własne zgodnie z zasadami nadawania haseł opisanych w Rozdziale III niniejszej instrukcji.

4. Dokument nadania lub usunięcia uprawnień musi być zawsze wypełniany w przypadku zmian zakresu uprawnień.
5. Karty uprawnień są przechowywane przez Administratora Bezpieczeństwa Informacji.
6. Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który po raz pierwszy korzysta z systemu informatycznego, odpowiada administrator sieci.
7. Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielany innej osobie.

III
Stosowane metody i środki uwierzytelniania użytkownika oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Użytkownik uzyskuje dostęp do danych osobowych przetwarzanych w systemie informatycznym wyłącznie po podaniu identyfikatora i hasła.
2. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik jest odpowiedzialny za wszystkie czynności wykonane przy użyciu swojego identyfikatora.
3. Identyfikator składa się minimalnie z 4 znaków, które nie są rozdzielone spacjami ani znakami interpunkcyjnymi. Identyfikator jest tworzony przy użyciu małych liter, z wyłączeniem polskich znaków.
4. Użytkownik, z chwilą przystąpienia do pracy w systemie informatycznym, otrzymuje hasło początkowe i jest zobowiązany zmienić je natychmiast po rozpoczęciu pracy, na sobie tylko znany ciąg znaków.
5. Hasło składa się co najmniej z 8 znaków.
6. Hasło powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
7. System informatyczny, który nie jest wyposażony w mechanizm wymuszający zmianę hasła po upływie 30 dni od dnia ostatniej jego zmiany, zobowiązuje użytkownika o cyklicznym co 30 dniowym zmianie tego hasła.
8. Hasło nie może być zapisane w miejscu dostępnym dla osób nieuprawnionych i należy je zachować w tajemnicy, również po upływie jego ważności.
9. Użytkownik nie może udostępniać osobom nieuprawnionym swojego identyfikatora oraz hasła. Po uwierzytelnieniu w systemie, użytkownik nie może udostępniać osobom nieuprawnionym swojego stanowiska pracy.
10. Jeśli istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest niezwłocznie je zmienić oraz powiadomić o tym fakcie.

IV

Rozpoczęcie, zawieszenie i zakończenie pracy przez użytkowników systemu

1. Użytkownik, rozpoczynając pracę na komputerze, loguje się do systemu informatycznego.
2. Dostęp do danych osobowych możliwy jest jedynie po dokonaniu uwierzytelnienia użytkownika.
3. Maksymalna liczba prób wprowadzenia hasła przy logowaniu się do systemu informatycznego wynosi 3. Po przekroczeniu tej liczby prób logowania system blokuje dostęp do zbioru danych na poziomie danego użytkownika. Odblokowania dostępu do zbioru danych może dokonać administrator sieci w porozumieniu z administratorem bezpieczeństwa informacji.
4. W przypadku braku aktywności użytkownika na komputerze przez czas dłuższy niż 10 minut następuje automatyczne włączenie wygaszacza ekranu.
5. Monitory stanowisk komputerowych, na których przetwarzane są dane osobowe, znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych, należy ustawić w taki sposób, aby uniemożliwić tym osobom wgląd w dane albo stosować blokowanie ekranu uniemożliwiające odczyt danych.
6. Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na obszarze, w którym są przetwarzane dane osobowe, jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania.
7. Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać na czas nieobecności osób upoważnionych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.
8. Przed opuszczeniem stanowiska pracy użytkownik jest obowiązany:
   1) wylogować się z systemu informatycznego

   albo

   2) wywołać blokowany hasłem wygaszacz ekranu.
9. Kończąc pracę użytkownik jest obowiązany:
   1) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy;
   2) zabezpieczyć stanowisko pracy.
10. Wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe, przechowuje się w szafach zamykanych na klucz.

V

Tworzenie kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu, poprzez tworzenie kopii zapasowych.

2. Za tworzenie kopii zapasowych zbiorów danych osobowych odpowiedzialny jest administrator sieci lub inna osoba przez niego wyznaczona.
3. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu informatycznego. Za przeprowadzanie tej procedury odpowiedzialny jest administrator sieci.
4. Kopie zapasowe wykonywane są zgodnie z następującym harmonogramem:
   1) kopia zapasowa aplikacji przetwarzającej dane osobowe – pełna kopia wykonywana jest w cykliczności comiesięcznej.
   2) kopia zapasowa danych osobowych przetwarzanych przez aplikację – pełna kopia wykonywana jest raz w tygodniu, a w przypadku wprowadzenia znacznych zmian danych osobowych, może być wykonywana częściej;
   3) kopia zapasowa danych konfiguracyjnych systemu informatycznego przetwarzającego dane osobowe, w tym uprawnień użytkowników systemu – pełna kopia wykonywana jest raz do roku.
5. Kopie zapasowe przechowywane są w szafie zamykanej na klucz.

VI
Sposób, miejsce i okres przechowywania elektronicznych nośników danych zawierających dane osobowe oraz kopii zapasowych

1. Użytkownicy nie mogą wynosić z terenu jednostki nośników danych z zapisanymi danymi osobowymi, bez zgody administratora danych osobowych lub administratora bezpieczeństwa informacji.
2. Okresowe kopie zapasowe wykonywane są na dyskietkach, płytach CD, DVD, taśmach lub innych nośnikach danych. Kopie przechowuje się w innych pomieszczeniach niż te, w których przechowywane są zbiory danych wykorzystywane na bieżąco. Kopie zapasowe przechowuje się w sposób uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie.
3. Dostęp do nośników z kopiami zapasowymi danych osobowych mają wyłącznie administrator danych oraz administrator sieci.
4. Usunięcie danych z systemu powinno zostać zrealizowane przy pomocy oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika danych.
5. Za zniszczenie kopii zapasowych sporządzanych indywidualnie przez użytkownika odpowiada użytkownik.
6. Dane osobowe w postaci elektronicznej należy usuwać z nośnika danych w sposób uniemożliwiający ich ponowne odtworzenie, nie później niż po upływie 5 dni po wykorzystaniu tych danych, chyba że z odrębnych przepisów wynika obowiązek ich przechowywania.
7. Nośniki danych podlegają komisyjnemu zniszczeniu w przypadku wycofania z eksploatacji

sprzętu komputerowego, na którym przetwarzane były dane osobowe, oraz po przeniesieniu danych osobowych do zbiorów danych w systemie informatycznym z nośników, których ponowne wykorzystanie nie jest możliwe. Z przeprowadzonych czynności komisja sporządza protokół.

8. Przez zniszczenie nośników danych należy rozumieć ich trwałe i nieodwracalne zniszczenie fizyczne do stanu uniemożliwiającego ich rekonstrukcję i odzyskanie danych.

VII

Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. Za ochronę antywirusową systemu informatycznego odpowiada administrator sieci.
2. System antywirusowy zainstalowany jest w każdym komputerze z dostępem do danych osobowych. Ustawienie poziomu bezpieczeństwa i wysyłanie aktualizacji bazy sygnatur wirusów zarządzane jest centralnie.
3. Programy antywirusowe są uaktywnione przez cały czas pracy każdego komputera w systemie informatycznym.
4. Wszystkie pliki otrzymywane z zewnątrz, jak również wysyłane na zewnątrz, podlegają automatycznemu sprawdzeniu przez system antywirusowy pod kątem występowania wirusów, z zastosowaniem najnowszej dostępnej wersji programu antywirusowego.
5. W przypadku pojawienia się wirusa, użytkownik obowiązany jest zaprzestać wykonywania jakichkolwiek czynności w systemie i niezwłocznie powiadomić o tym fakcie administratora sieci lub administratora bezpieczeństwa informacji.
6. Niedozwolone jest otwieranie wiadomości poczty elektronicznej i załączników od „niezaufanych" nadawców.
7. Niedozwolone jest wyłączanie, blokowanie i odinstalowywanie programów zabezpieczających komputer przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem (skaner antywirusowy, firewall).
8. Administrator sieci jest odpowiedzialny za aktywowanie i poprawne konfigurowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku:
   1) sieci lokalnej i rozległej;
   2) stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.

VIII
Udostępnianie danych osobowych i sposób odnotowywania informacji o udostępnianiu danych

1. Dane osobowe przetwarzane w jednostce mogą być udostępnione osobom lub podmiotom uprawnionym do ich otrzymania, na mocy ustawy o ochronie danych osobowych oraz innych przepisów powszechnie obowiązujących.
2. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepisy odrębne stanowią inaczej.
3. Dane udostępnione jednostce przez inny podmiot można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
4. Administrator danych prowadzi ewidencję udostępnionych danych, która zawiera:
   1) numer ewidencyjny wydruku;
   2) zakres udostępnionych danych;
   3) adresata udostępnionych danych;
   4) datę udostępnienia.
5. Odnotowanie informacji powinno nastąpić niezwłocznie po udostępnieniu danych.

IX
Wykonywanie przeglądów i konserwacji systemu oraz nośników danych służących do przetwarzania danych

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe mogą być wykonywane przez firmy zewnętrzne pod nadzorem administratora sieci.
2. Administrator sieci okresowo sprawdza możliwość odtworzenia danych z kopii zapasowej. Częstotliwość wykonywania procedury odtwarzania danych jest uzgadniana z administratorem bezpieczeństwa informacji.
3. Aktualizacja oprogramowania powinna być przeprowadzana zgodnie z zaleceniami producentów oraz opinią rynkową, co do bezpieczeństwa i stabilności nowych wersji.
4. Za terminowość przeprowadzania przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada administrator sieci.
5. Nieprawidłowości w działaniu systemu informatycznego oraz oprogramowania są niezwłocznie usuwane przez administratora sieci lub firmę zewnętrzną pod nadzorem administratora sieci, a ich przyczyny analizowane.
6. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana

jego lokalizacji, może być dokonana tylko za wiedzą i zgodą administratora bezpieczeństwa informacji.

X

Postępowanie w przypadku naruszenia ochrony danych osobowych

1. Każdy użytkownik, który stwierdza lub podejrzewa naruszenie ochrony danych w systemie informatycznym, zobowiązany jest niezwłocznie poinformować o tym administratora sieci.
2. Do czasu przybycia administratora sieci na miejsce naruszenia lub ujawnienia naruszenia ochrony danych osobowych, należy:
   1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców naruszenia;
   2) rozważyć wstrzymanie bieżącej pracy na komputerze w celu zabezpieczenia miejsca zdarzenia;
   3) zaniechać, o ile to możliwe, dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę;
   4) udokumentować wstępnie zaistniałe naruszenie;
   5) nie opuszczać, bez uzasadnionej potrzeby, miejsca zdarzenia do czasu przybycia administratora sieci lub administratora bezpieczeństwa informacji.
3. Po przybyciu na miejsce naruszenia lub ujawnienia naruszenia ochrony danych osobowych administrator sieci:
   1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania;
   2) może żądać wyjaśnień dotyczących zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem;
   3) dokonuje zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się skutków naruszenia;
   4) podejmuje odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia;
   5) rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu administratora danych osobowych.
4. Po wyczerpaniu niezbędnych środków doraźnych, administrator sieci zasięga niezbędnych opinii i proponuje działania mające na celu usunięcie naruszenia i jego skutków oraz ustosunkowuje się do kwestii ewentualnego odtworzenia danych z kopii zapasowej i terminu wznowienia przetwarzania danych.

5. Administrator danych osobowych dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który zawiera w szczególności:
   1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób, które złożyły wyjaśnienia w związku z naruszeniem;
   2) określenie czasu i miejsca naruszenia oraz powiadomienia o naruszeniu;
   3) określenie rodzaju naruszenia i okoliczności mu towarzyszących;
   4) wyszczególnienie uwzględnionych przesłanek wyboru metody postępowania i opis podjętego działania;
   5) wstępną ocenę przyczyn wystąpienia naruszenia;
   6) ocenę przeprowadzonego postępowania wyjaśniającego i działań podjętych w celu usunięcia naruszenia i jego skutków.
6. Administrator danych osobowych przekazuje raport kierownikowi jednostki w terminie 14 dni od daty zdarzenia.
7. Po przywróceniu prawidłowego funkcjonowania systemu informatycznego, administrator sieci przeprowadza szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia oraz podejmuje kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

Sporządził	*Zatwierdził:*
Administrator Bezpieczeństwa Informacji	*Administrator Danych Osobowych*
……..	…….