

ZARZĄDZENIE NR 0152/12/2010
WÓJTA GMINY JASZENICA
z dnia 15 grudnia 2010 roku

w sprawie: wprowadzenia instrukcji dotyczącej ochrony danych osobowych zlokalizowanych w systemie informatycznym Urzędu Gminy Jasienica.

Na podstawie art. 31 oraz art. 33 ust. 3, w związku z art. 11a ust. 1 pkt. 2 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (tj. Dz.U. z 2001r. Nr 142, poz. 1591, z późn. zm.), art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz.U. z 2002r. Nr 101, poz. 926 z późn. zm.) oraz § 3 i § 5 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. Nr 100, poz. 1024)

zarządzam co następuje:

§ 1

Wprowadzić „Instrukcję zarządzania systemem informatycznym w Urzędzie Gminy Jasienica” w brzmieniu stanowiącym załącznik do niniejszego zarządzenia.

§ 2

Zobowiązuje się pracowników Urzędu Gminy Jasienica dopuszczonych upoważnieniem do przetwarzania danych osobowych do przestrzegania postanowień dokumentu o którym mowa w § 1.

§ 3

Zobowiązuje się kierowników referatów Urzędu Gminy w Jasienicy w których przetwarzane są dane osobowe do sprawowania nadzoru nad ich ochroną. Zapis ten dotyczy również pracowników na stanowiskach samodzielnych.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

RADCA PRAWNY

Magdalena Maria Kubica
KTB 414

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM W URZĘDZIE GMINY JASIENICA

Podstawa prawna.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz rozporządzenie 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. Nr 100, poz. 1024 z późn. zm.)

Postanowienia ogólne.

§ 1

Instrukcja zarządzania systemem informatycznym w Urzędzie Gminy Jasienica jest wewnętrznym dokumentem eksploatacyjnym regulującym i opisującym zasady oraz procedury pracy, zarządzania i administrowania systemem informatycznym Urzędu Gminy Jasienica.

Określenia i skróty użyte w instrukcji zarządzania oznaczają:

1. Administrator Danych Osobowych – Wójt Gminy Jasienica, zwany dalej Administratorem.
2. ABI - Administrator Bezpieczeństwa Informacji – osoba wyznaczona przez Administratora, w rozumieniu art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.), dalej zwana Ustawą.
3. ASI - Administrator Systemów Informatycznych – pracownicy wyznaczeni przez Administratora odpowiedzialni za wdrożenie i stosowanie zasad bezpieczeństwa systemów informatycznych, zobowiązani do stosowania technicznych i organizacyjnych środków ochrony przewidzianych w systemach informatycznych.
4. Użytkownik systemu – osoba posiadająca upoważnienie do wprowadzania i przetwarzania danych w systemie informatycznym w zakresie wskazanym w upoważnieniu.

5. Przełożony użytkownika, zwany dalej przełożonym – Zastępca Wójta, Sekretarz, Skarbnik, Kierownicy referatów - osoby odpowiedzialne za przestrzeganie zasad przetwarzania i ochrony danych przez podległych im pracowników.
6. Hasło – ciąg znaków literowych, cyfrowych lub innych specjalnych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
7. Identyfikator użytkownika - ciąg znaków literowych, cyfrowych lub innych specjalnych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w systemie informatycznym.
8. Sieć LAN/WAN – sieć lokalna/rozległa wykorzystująca specjalistyczne dedykowane urządzenia sieci telekomunikacyjnych w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.).
9. Połączenie VPN – wirtualna sieć prywatna, w której transmitowane dane są szyfrowane celem zwiększenia bezpieczeństwa tych danych.
10. Rejestr udostępnionych danych osobowych, zwany dalej Rejestrem – rejestr, w którym odnotowywane są informacje o odbiorcach danych z systemu/aplikacji, prowadzony dla danego systemu/aplikacji.

Procedury nadawania, zmiany uprawnień do przetwarzania danych

§ 2

1. Każdy użytkownik systemu informatycznego przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:
 - a) niniejszą instrukcją,
 - b) Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101, poz. 926 z późn. zm.).
2. Pracownik potwierdza własnoręcznym podpisem zapoznanie się i zrozumienie treści wynikających z powyższych informacji na oświadczeniu, którego wzór stanowi załącznik nr 1.
3. Podstawą nadania uprawnień dostępu do systemu informatycznego jest wypełniony wniosek przełożonego stanowiący załącznik nr 2.
4. Opis procedury nadawania/odbierania uprawnień dostępu do lokalnej sieci komputerowej realizowany jest zgodnie z poniższymi zasadami. Użytkownicy uzyskują dostęp do sieci na z góry zdefiniowanym poziomie użytkownika zgodnie z powierzonymi zadaniami i obowiązkami na danym stanowisku.
5. Procedura nadania/odebrania uprawnień użytkownikowi jest następująca:

- a) przełożony użytkownika wnioskuje o nadanie/odebranie uprawnień do przetwarzania danych w systemie informatycznym eksploatowanym w Urzędzie Gminy Jasienia.
 - b) zgłasza do ASI konieczność nadania/odebrania uprawnień użytkownikowi na wymaganym poziomie w systemie informatycznym na formularzu stanowiącym załącznik nr 2. do Instrukcji Zarządzania.
 - c) ASI po otrzymaniu wypełnionego formularza tworzy/usuwa użytkownika o unikalnym identyfikatorze w systemie informatycznym i nadaje mu hasło początkowe oraz wymagane uprawnienia (zakres dostępnych danych i operacji).
 - d) w przypadku wnioskowanej przez przełożonego zmiany w posiadanych uprawnieniach użytkownika, ASI zobowiązany jest do zablokowania odbieranych użytkownikowi uprawnień lub nadania nowych.
 - e) po wykonaniu powyższych czynności ASI jest zobowiązany poinformować przełożonego użytkownika o nadaniu/odebraniu wnioskowanych uprawnień.
 - f) użytkownik podczas pierwszego logowania do systemu informatycznego zobowiązany jest zmienić predefiniowane hasło ustawione przez ASI na indywidualne hasło.
6. Powyższą procedurę nadawania/odbierania uprawnień do przetwarzania danych w systemie informatycznym należy stosować zarówno w przypadku nowych użytkowników podczas nadawania/odbierania uprawnień jak i do zmiany posiadanych przez użytkownika uprawnień.

Zasady uwierzytelniania w systemie informatycznym oraz procedury związane z ich zarządzaniem i użytkowaniem

§ 3

- 1. Podstawową zasadą bezpieczeństwa systemu informatycznego Urzędu Gminy Jasienica jest ochrona informacji przed nieuprawnionym dostępem, ujawnieniem, nieautoryzowanym usunięciem lub modyfikacją danych.
- 2. Stosowane środki ochrony danych w postaci zasad uwierzytelniania i procedury nadawania/odbierania/zmiany uprawnień użytkowników w systemie informatycznym mają na celu zapewnienie poufności, integralności i rozliczalności danych.
- 3. Użytkownik posiadający uprawnienia do przetwarzania danych w systemie informatycznym ponosi pełną odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła.
- 4. W systemie informatycznym Urzędu Gminy Jasienica stosowana jest procedura dwustopniowego logowania:

- a) poziom pierwszy – logowanie do systemu operacyjnego i sieci LAN/WAN
 - b) poziom drugi – logowanie do aplikacji dziedzinowych
5. Każdy użytkownik posiada unikalny nadawany przez ASI identyfikator osobowy.
6. Hasło do identyfikatora użytkownik powinien tworzyć zgodnie z zasadami:
- a) minimalna długość hasła – 8 znaków ,
 - b) zakazuje się stosować: haseł, które użytkownik stosował uprzednio, swojego identyfikatora w jakiegokolwiek formie, swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiegokolwiek formie, imion (w szczególności imion osób z najbliższej rodziny), ogólnie dostępnych informacji o użytkowniku(numer telefonu, numer rejestracyjny samochodu, numeru PESEL, itp.),
 - c) należy stosować: hasła zawierające kombinacje liter i cyfr, hasła zawierające znaki specjalne: (.,()';@, #, & itp.) o ile system informatyczny i oprogramowanie na to pozwala,
 - d) zmiany hasła nie wolno zlecać innym osobom,
 - e) hasło nie może być ujawnione innej osobie nawet po utracie jego ważności,
 - f) system automatycznie powinien wymuszać zmianę hasła nie rzadziej, niż jeden raz w miesiącu,
 - g) hasło musi być niezwłocznie zmienione przez użytkownika w przypadku podejrzenia lub stwierdzenia jego ujawnienia.

Procedury rozpoczęcia, zawieszania i zakończenia pracy przez użytkowników systemu

§ 4

1. Rozpoczęcie pracy w systemie informatycznym wymaga zalogowania się użytkownika do systemu operacyjnego za pomocą indywidualnego identyfikatora użytkownika oraz jego hasła.
2. W przypadku trzy krotnego podania złego hasła dany identyfikator zostanie automatycznie zablokowany. Po zablokowaniu identyfikatora, użytkownik powinien niezwłocznie o tym fakcie poinformować ASI. Odblokowanie identyfikatora dokonuje ASI wraz ze zmianą hasła na hasło początkowe oraz wymuszeniem zmiany hasła podczas pierwszego logowania użytkownika.
3. Po zalogowaniu się do systemu operacyjnego użytkownik systemu może uruchamiać aplikacje dziedzinowe zgodnie z nadanymi przez ASI uprawnieniami.
4. Uruchomienie wszystkich aplikacji dziedzinowych odbywa się analogicznie z logowaniem użytkownika do systemu operacyjnego.
5. Użytkownik podczas opuszczenia stanowiska komputerowego, na którym jest zalogowany zobowiązany jest do zablokowania komputera.

6. Zakończenie pracy w systemie informatycznym polega na:
- a) zamknięciu wszystkich programów dziedzinowych,
 - b) wylogowaniu się użytkownika z systemu operacyjnego,
 - c) zamknięciu systemu operacyjnego,
 - d) wyłączeniu komputera oraz monitora

**Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi
programowych służących do ich przetwarzania**

§ 5

1. Kopie zapasowe mają na celu zapewnienie ciągłości pracy w systemie informatycznym po ewentualnej jego awarii oraz w przypadku potrzeby analizy danych archiwalnych.
2. Kopie zapasowe wykonywane są w następujących cyklach:
 - a) w cyklu dziennym wykonywane są automatyczne kopie zapasowe wszystkich baz danych znajdujących się w systemie informatycznym Urzędu Gminy Jasienica
 - b) w cyklu tygodniowym wykonywana jest automatyczna kopia zapasowa wszystkich aplikacji dziedzinowych oraz plików użytkowników przechowywanych na sieciowym serwerze plików wraz z kompletem dziennych kopii zapasowych baz danych.
 - c) w cyklu tygodniowym ASI nagrywa utworzone powyżej kopie zapasowe na elektroniczne nośniki DVD-R.
3. Po nagraniu kopii zapasowej na nośniki DVD-R, ASI ma obowiązek opisać te nośniki za pomocą daty wykonania kopii, numeru płyty danej kopii zapasowej oraz kolejnym numerem kopii.
4. Fakt nagrania kopii zapasowej na elektroniczne nośniki DVD-R musi zostać potwierdzony wpisem na formularzu „Kontroli wykonania tygodniowej kopii zapasowej”, którego treść stanowi załącznik nr 3.

**Przechowywanie elektronicznych nośników informacji zawierających dane osobowe oraz
kopii zapasowych**

§ 6

1. Elektroniczne nośniki informacji.
 - a) Dane osobowe w postaci elektronicznej - za wyjątkiem kopii bezpieczeństwa - zapisane na dyskietkach, płytach CD/DVD, dyskach twardych w tym na dyskach zewnętrznym

typu PenDrive nie mogą opuścić obszaru przetwarzania danych osobowych wskazanego w załączniku nr 4.

- b) elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszary przetwarzania danych osobowych zgodnie z załącznikiem nr 4, w zamkniętych na klucz szafach,
- c) wszystkie elektroniczne nośniki informatyczne zawierające dane osobowe, przeznaczone do likwidacji muszą zostać uszkodzone mechanicznie w sposób uniemożliwiający odczyt z nich danych,
- d) elektroniczne nośniki informacji, zawierające dane osobowe, nie mogą zostać przekazane innemu podmiotowi nieuprawnionemu do ich dostępu,
- e) sprzęt komputerowy przekazywany do naprawy musi zostać pozbawiony elektronicznych nośników informacji zawierających dane osobowe.

2. Kopie zapasowe:

- a) kopie zapasowe są przechowywane w szafie zlokalizowanej w serwerowni Urzędu Gminy Jasienica na I piętrze,
- b) okres przechowywania kopii zapasowych wynosi 5 lat od daty ich utworzenia

Środki ochrony systemu informatycznego

§ 7

1. System informatyczny eksploatowany w Urzędzie Gminy Jasienica jest chroniony przed:

- a) wirusami i szkodliwym oprogramowaniem,
- b) nieuprawnionym dostępem do sieci LAN,
- c) awarią zasilania elektrycznego,

2. Ochrona przed wirusami i szkodliwym oprogramowaniem:

- a) na każdym stanowisku komputerowym w tym również na każdym serwerze musi być zainstalowane oprogramowanie antywirusowe,
- b) oprogramowanie antywirusowe jest centralnie zarządzane i automatycznie aktualizowane z poziomu serwera zarządzającego,
- c) aktualizacja programu antywirusowego oraz definicji wirusów odbywa się nie rzadziej niż raz w tygodniu,
- d) oprogramowanie antywirusowe ma zawsze włączoną ochronę antywirusową i antyspyware oraz ochronę systemu plików w czasie rzeczywistym,

- e) dostęp do zaawansowanej konfiguracji oprogramowania antywirusowego i antyspyware zabezpieczony jest przez ASI hasłem, uniemożliwiając w ten sposób użytkownikowi wprowadzenia zmian w jego konfiguracji,
- f) za poprawną instalację i konfigurację oprogramowania antywirusowego i antyspyware na komputerach oraz serwerach w lokalnej sieci komputerowej Urzędu Gminy Jasienica odpowiedzialny jest ASI, bez jego zgody użytkownik nie może instalować i odinstalowywać wyżej wymienionego oprogramowania, ani zmieniać jego konfiguracji.

3. Ochrona przed nieuprawnionym dostępem do sieci LAN:

- a) dostęp z sieci Internet do sieci LAN Urzędu Gminy Jasienica chroniony jest przez router z aktywną funkcją firewall,
- b) ASI może udzielić użytkownikowi dostęp z sieci Internet do sieci LAN zestawiając na tą potrzebę szyfrowany wirtualny kanał sieciowy VPN,
- c) użytkownikowi nie wolno samodzielnie podłączać i odłączać do sieci LAN stacjonarnego i przenośnego sprzętu komputerowego oraz urządzeń sieciowych.

4. Ochrona przed awarią zasilania elektrycznego:

system, w którym przetwarzane są dane osobowe powinien posiadać mechanizm zasilania awaryjnego UPS, zabezpieczając w ten sposób system przed nieautoryzowaną zmianą napięcia.

Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych.

§ 8

- 1. Dane osobowe znajdujące się w systemie informatycznym mogą być udostępniane wyłącznie osobom do tego uprawnionym.
- 2. Udostępnianie nie może odbywać się drogą telefoniczną.
- 3. Użytkownicy systemu informatycznego nie mogą wnosić poza obszar przetwarzania danych żadnych zbiorów danych

Procedury wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych.

§ 9

- 1. Dla zachowania ciągłości pracy i bezpieczeństwa danych przeprowadza się okresowe przeglądy i konserwacje systemu informatycznego. Czynności te obejmują zarówno platformy sprzętowe jak i oprogramowanie służące do przetwarzania danych osobowych.

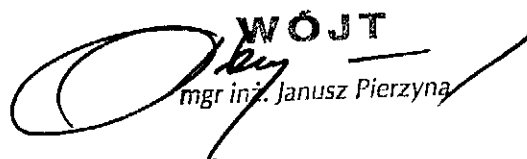
2. Przegląd i konserwacja platformy sprzętowej:

- a) przeglądy i konserwacje sprzętu powinny być wykonywane w terminach określonych przez producenta sprzętu,
- b) jeżeli producent sprzętu nie określa terminów wykonywania przeglądów i konserwacji sprzętu o terminach tych decyduje ASI,
- c) wszelkie nieprawidłowości wykazane podczas przeglądów i konserwacji powinny być niezwłocznie usunięte, a przyczyny tych nieprawidłowości powinny zostać przeanalizowane,

3. Przegląd i konserwacja oprogramowania:

- a) oprogramowanie służące do przetwarzania danych osobowych powinno być aktualizowane i konserwowane zgodnie z wytycznymi producenta,
- b) w przypadku wykrycia przez użytkownika błędów lub błędu w działaniu oprogramowania służącego do przetwarzania danych użytkownik powinien niezwłocznie o tym fakcie powiadomić ASI oraz ABI,
- c) ASI po otrzymaniu informacji o wadliwym działaniu programu powinien o tym fakcie powiadomić producenta oprogramowania, a także o ile to możliwe powrócić do wersji programu w której dany błąd nie występował.

4. Przegląd i konserwacja nośników informacji odbywa się na tych samych zasadach co przegląd i konserwacja platformy sprzętowej.


WÓJT
mgr inż. Janusz Pierzyna

OŚWIADCZENIE

Ja niżej podpisany(a) ... oświadczam, że zostałem(am) zapoznany(a) i zrozumiałem(am) treści wynikające z przepisów dotyczących ochrony danych osobowych, w tym z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.), rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) oraz zarządzeniem Nr /2010 Wójta Gminy Jasienica z dnia w sprawie wprowadzenia do użytku służbowego instrukcji dotyczącej ochrony danych osobowych w Urzędzie Gminy Jasienica.

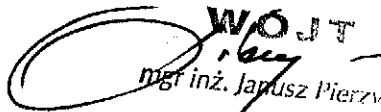
Zobowiązuję się do zachowania w tajemnicy danych osobowych, do których mam i będę miał(a) dostęp w związku z wykonywaniem przeze mnie zadań służbowych i obowiązków pracowniczych w Urzędzie Gminy Jasienica, zarówno w trakcie obecnie wiążącego mnie stosunku pracy jak i po ustaniu zatrudnienia.

Zobowiązuję się przestrzegać regulaminów, instrukcji i procedur obowiązujących w Urzędzie Gminy Jasienica dotyczących ochrony danych osobowych, a w szczególności, że nie będę bez pisemnego upoważnienia służbowego wykorzystywał(a) danych osobowych ze zbiorów Urzędu Gminy Jasienica

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane za naruszenie obowiązków pracowniczych w rozumieniu Kodeksu Pracy.

Jasienica, dnia

.....
podpis osoby składającej oświadczenie


mgr inż. Janusz Pierzyna

WNIOSEK O NADANIE UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM.

<input type="checkbox"/> Nowy użytkownik	<input type="checkbox"/> Zmiana uprawnień	<input type="checkbox"/> Odebranie uprawnień
--	---	--

Imię i Nazwisko użytkownika	
Wydział	
Pokój	
Numer telefonu	
Użytkownik posiada uprawnienie do przetwarzania danych osobowych	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
Opis zakresu uprawnień użytkownika w systemie informatycznym: (proszę wpisać nazwy programów do których użytkownik powinien mieć dostęp)	
Dostęp do Internetu:	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
Poczta elektroniczna:	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
Podpis zgłaszającego wniosek (przełożonego)	
Podpis nadającego uprawnienia (ASD)	
Data nadania uprawnień	

WOJT
mgr inż. Janusz Pierzyna

KONTROLA WYKONANIA TYGODNIOWEJ KOPII BEZPIECZEŃSTWA

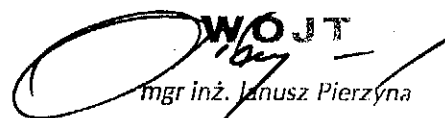
[illegible]

WOJT
mgr inż. Janusz Pierzyń

**WYKAZ POMIESZCZEŃ W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE
Z UŻYCIEM STACJONARNEGO SPRZĘTU KOMPUTEROWEGO**

LOKALIZACJA	Nr pokoju
parter	3
I piętro	101, 102, 103, 104, 105, 106, 107A, 107B, 108, 109, 110, 111, 112, 116, 117, 118, 119, 120, 121, 123, 124, 126, 127
II piętro	201, 202, 203, 204, 205, 206

Wszystkie pomieszczenia znajdujące się w wykazie zlokalizowane są w budynku Urzędu Gminy Jasienica w Jasienicy 159, 43-385


mgr inż. Janusz Pierzyna