URZĄD GMINY w Słupnie
09-472 Słupno, ul. Miszewska 8a
Reg. 000539029, NIP: 774-22-93-320
tel. (024) 261 29 77

OZ.0050.79.2012

ZARZĄDZENIE NR 79/2012
Wójta Gminy w Słupnie
z dnia 1 października 2012 r.

w sprawie „Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Gminy Słupno"

Na podstawie § 3 ust.3 i § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 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), zarządza się co następuje:

§1

Wprowadza się „Instrukcję Zarządzania Systemem Informatycznym w Urzędzie Gminy Słupno", zwana dalej Instrukcją. Treść instrukcji zawiera załącznik do zarządzenia.

§2

Instrukcja, o której mowa w §1 ma zastosowanie na wszystkich stanowiskach pracy gdzie przetwarzane są dane osobowe.

§3

Zobowiązuje się pracowników Urzędu do stosowania zasad określonych w instrukcji.

§4

Traci moc zarządzenie Nr 52/2006 Wójta Gminy Słupno z dnia 29 grudnia 2006 roku w sprawie ustalenia „Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Gminy Słupno".

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
mgr Stefan Jakubowski

RADCA PRAWNY
mgr Henryk Nowakowski
WR-P-147

WÓJT
mgr Stefan Jakubowski

Załącznik nr 1 do Zarządzenia nr 79/2012
Wójta Gminy Słupno z dnia 1 października 2012 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM URZĘDU GMINY SŁUPNO

Słupno 2012r.

SPIS TREŚCI

I. Postanowienia ogólne

§1

Instrukcja określa procedury zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwanych dalej danymi, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji w Urzędzie Gminy w Słupnie zwanym dalej Urzędem.

§2

Instrukcja w szczególności zawiera:

1. określenie procedury przydziału haseł dla użytkowników i częstotliwość ich zmiany, ze wskazaniem osoby odpowiedzialnej za te czynności,
2. określenie procedury rejestrowania i wyrejestrowywania użytkowników oraz wskazanie osoby odpowiedzialnej za te czynności,
3. procedury rozpoczęcia i zakończenia pracy w systemach informatycznych,
4. opis metod oraz procedurę i harmonogram tworzenia kopii bezpieczeństwa,
5. opis metod i harmonogram sprawdzania obecności wirusów komputerowych oraz metody ich usuwania,
6. procedurę i okres przechowywania elektronicznych nośników informacji i wydruków,
7. procedurę i harmonogram dokonywania przeglądów i konserwacji systemów oraz zbiorów danych osobowych,
8. procedury zakupu, eksploatacji oraz utylizacji stacji roboczych
9. procedury zakupu, instalacji i aktualizacji oprogramowania.

§3

Określenia użyte w instrukcji oznaczają:

1. **Ustawa** – Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002r. Nr 101 poz. 926, ze zm.),
2. **Rozporządzenie** – Rozporządzenie Rozporządzeniem 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. 2004r. Nr 100 poz. 1024),
3. **Urząd** – Urząd Gminy w Słupnie,
4. **Komórka organizacyjna** – odpowiednio referaty, samodzielne stanowiska pracy.
5. **Administrator Danych** – Wójt Gminy Słupno,
6. **ABI** - Administrator Bezpieczeństwa Informacji,
7. **Administrator Systemu Informatycznego (ASI)** – osoba odpowiedzialna za funkcjonowanie systemu informatycznego Urzędu oraz stosowanie technicznych i organizacyjnych środków ochrony.
8. **Sieć lokalna** – połączenie systemów informatycznych urzędu wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych
9. **Sieć rozległa** – sieć publiczna w rozumieniu ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852 z późn. zm.)
10. **Użytkownik systemu** zwany dalej użytkownikiem - osoba upoważniona do przetwarzania danych osobowych w systemie informatycznym urzędu także osoba przetwarzająca dane w toku wykonywania umowy cywilnoprawnej zawartej z Urzędem (np. umowy zlecenia, umowy o dzieło, itp.) , pracownik innego podmiotu, który świadczy usługi związane z pracą w systemie Urzędu, na podstawie odrębnych umów z tym podmiotem (np. serwis, zlecenie przetwarzania danych, itp.)

§4.

1. Ochrona zasobów danych Urzędu jako całości, przed ich nieuprawnionym użyciem lub zniszczeniem, jest jednym z podstawowych obowiązków każdego pracownika Urzędu.
2. Obowiązkiem każdego pracownika Urzędu jest zachowanie tajemnicy służbowej, w tym ochrony danych osobowych gromadzonych i przetwarzanych przez Urząd. Obowiązek ten istnieje również po ustaniu zatrudnienia.
3. Osoby zatrudnione przy przetwarzaniu danych (także poza systemem) są zobowiązane do szczególnej dbałości o zachowanie poufności, integralności i ograniczenie dostępności do danych gromadzonych w kartotekach, skorowidzach itp. oraz infrastruktury sprzętowo – programowej systemu.

§5.

1. Za bezpieczeństwo danych osobowych Urzędu, odpowiadają:
   1) Administrator danych osobowych – Wójt Gminy Słupno,
   2) Administrator Bezpieczeństwa Informacji Urzędu.

§6.

Obowiązki wynikające z ustawy o ochronie danych osobowych Wójt Gminy Słupno powierza kierownikom referatów - w zakresie podległych im pracowników.

§7.

1. Obszary przetwarzania danych w obiektach i pomieszczeniach Urzędu nie mogą być dostępne dla osób nieuprawnionych.
2. W pomieszczeniach, w których przyjmowani są interesanci należy stosować szczególne środki ostrożności, w tym:
   1) interesanci powinni wchodzić pojedynczo i pozostawać w pomieszczeniu tylko w obecności użytkownika systemu,
   2) kartoteki tradycyjne należy zabezpieczyć przed dostępem osób nieuprawnionych,
   3) nie należy pozostawiać dokumentów papierowych i nośników elektronicznych w miejscach umożliwiających ich wykorzystanie, przez osoby nieuprawnione,
   4) monitory powinny być usytuowane tak, aby ekrany były niewidoczne dla osób nieuprawnionych,
   5) drukarki i urządzenia peryferyjne powinny być usytuowane tak, aby znajdowały się z dala od przestrzeni, po której poruszają się osoby nieuprawnione,

§8.

Systemy informatyczne w Urzędzie powinny być tak zaprojektowane, aby wymuszać autoryzację osoby przystępującej do pracy na zbiorach danych osobowych.

§9.

Odpowiedzialność za ochronę danych zawartych na komputerach przenośnych i innych przenośnych urządzeniach umożliwiających gromadzenie danych, spoczywa wyłącznie na dysponentach tych urządzeń; minimalnym wymaganym zabezpieczeniem każdego komputera PC w Urzędzie jak również komputera przenośnego jest ograniczenie dostępu do tego komputera hasłem (hasło na BIOS, Windows, wygaszasz ekranu).

§10.

1. **Zabrania się:**
   1) zapisywania indywidualnych haseł dostępu,
   2) dokonywania samowolnych napraw sprzętu informatycznego oraz modyfikowania oprogramowania,
   3) samodzielnego zakupu sprzętu komputerowego lub oprogramowania bez wiedzy i akceptacji Administratora Systemu Informatycznego,
   4) autoryzacji w systemie jako inny użytkownik,
   5) samodzielnego wgrywania oprogramowania,
   6) w celach innych niż służbowe, wynoszenia dokumentacji, w tym na nośnikach elektronicznych zawierającej dane, poza obszar jednostki organizacyjnej,
   7) instalowania na komputerach Urzędu prywatnych kont poczty elektronicznej,
   8) wykorzystywania Internetu do celów innych niż służbowe oraz przeglądania stron o tematyce pornograficznej, nielegalnych stron z kodami aktywacyjnymi do programów lub programami łamiącymi zabezpieczenia programów przed nielegalnym kopiowaniem.
   9) korzystania z czatów internetowych, ściągania plików muzycznych oraz filmów.

II. Procedury rejestrowania i wyrejestrowywania użytkowników

§11.

1. Pracownika Urzędu korzystającego z systemu i jego oprogramowania rejestruje się jako użytkownika.
2. Niedopuszczalna jest praca w systemie na koncie innego użytkownika.

§12.

1. W celu zarejestrowania osoby jako użytkownika systemu, kierownik referatu Urzędu w którym zatrudniona jest osoba, bądź Wójt w przypadku osób zatrudnionych na samodzielnych stanowiskach, zwraca się do ASI o nadanie koniecznych uprawnień
2. Administrator Systemu Informatycznego w porozumieniu z Administratorem Bezpieczeństwa Informacji nadaje, nadzoruje i wycofuje uprawnienia.
3. Dostęp do poszczególnych elementów systemów bazodanowych powinien być realizowany tylko w zakresie określonym nadanymi uprawnieniami, po wydaniu upoważnienia użytkownikowi

§13.

Identyfikator użytkownika powinien spełniać następujące wymagania:

1. długość minimum trzy znaki,
2. musi być niepowtarzalny w skali systemu,
3. jednym identyfikatorem może posługiwać się tylko jeden użytkownik,
4. identyfikator jest natychmiast blokowany przez Administratora Systemu Informatycznego po rozwiązaniu z pracownikiem umowy o pracę, po uzyskaniu takiej informacji z kadr,
5. identyfikator pracownika, który rozwiązał umowę o pracę nie może zostać przydzielony innemu pracownikowi.

§14.

1. Identyfikator i hasło osoby, która utraciła uprawnienia do korzystania z systemu należy bezzwłocznie unieważnić.
2. Identyfikator osoby, która utraciła uprawnienia i została wyrejestrowana z systemu nie może być przydzielony innej osobie.

III. Budowa i procedura przydziału haseł dla administratorów systemów i użytkowników oraz częstotliwość ich zmiany

§15.

Określa się następujące zasady tworzenia haseł.

1. Hasło musi mieć nie mniej niż 8 znaków.
2. Hasło powinno zawierać znaki z wszystkich trzech niżej wymienionych grup:
   a) małe i duże litery,
   b) cyfry,
   c) znaki specjalne.
4. W haśle nie wolno używać :
   a) swojej nazwy użytkownika;
   b) swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie;
   c) ogólnie dostępnych informacji o użytkowniku tj: nr telefonu, nr rejestracyjny samochodu, jego marki, nr dowodu, nazwa ulicy itp.
   d) wyrazów słownikowych,
   e) przewidywanych sekwencji znaków kławiatury tj; „12345678" itp.
5. Hasło jest obowiązkowe dla każdego użytkownika, posiadającego identyfikator w systemie.
6. Po założeniu hasła przez ASI użytkownik ma obowiązek zarejestrować się do systemu i zmienić hasło.

§16.

Określa się następujące zasady korzystania z haseł:

1. Nie wolno powtórnie używać hasła raz użytego.
2. Hasło znane jest tylko użytkownikowi.
3. Przy wpisywaniu hasła nie jest ono wyświetlane na ekranie.
4. Użytkownik odpowiada za systematyczną zmianę haseł.
5. Użytkownik powinien wszystkie używane przez niego hasła do systemów i programów spisać i zapieczętowane w podpisanej kopercie oznaczone datą po comiesięcznej zmianie przekazać Administratorowi Bezpieczeństwa Informacji.

§17.

Niedopuszczalne jest podawanie swojego hasła innym użytkownikom bądź osobom nie uprawnionym do pracy w systemie lub nie posiadającym uprawnień do przetwarzania danych.

§18.

1. Hasła w systemach Urzędu zmienia się nie rzadziej niż raz w miesiącu.
2. Powyższe zalecenie jest obowiązujące w Urzędzie niezależnie od tego czy użytkownik przetwarza dane.

§19.

1. ASI tworzy i zmienia hasła zgodnie z zasadami określonymi w niniejszej Instrukcji.
2. Hasła do serwera, aktywnych urządzeń sieci i istotnych programów konfiguracyjnych, Administrator Systemu Informatycznego umieszcza w zapieczętowanych kopertach i zabezpiecza w obecności Administratora Bezpieczeństwa Informacji.
3. Otwarcie koperty określonej w §16 ust.5 oraz §19 ust. 2 może nastąpić w przypadku:
   1) kontroli,
   2) zamiaru zniszczenia nieaktualnych haseł przez Administratora Systemu Informatycznego,
   3) zaistnienia konieczności zapoznania się z jej zawartością spowodowanej rezygnacją z pracy, pozbawieniem uprawnień lub śmiercią ASI; uprawnienie w tym zakresie posiada Administrator Bezpieczeństwa Informacji,
   4) innym określonym w rozdziale VII „Polityki Przetwarzania Danych Osobowych w Urzędzie Gminy Słupno"

IV. Procedura rozpoczęcia i zakończenia pracy w systemie informatycznym

§20.

1. Włączając komputer w celu podjęcia pracy użytkownik dokonuje autoryzacji zgodnie z poleceniami wydawanymi przez system komputerowy ukazującymi się na ekranie monitora.
2. W przypadku pojawienia się trudności w autoryzacji, pomimo prawidłowo wykonanych czynności, użytkownik zobowiązany jest skontaktować się z Administratorem Systemu Informatycznego.
3. Jeżeli autoryzacja przebiegła prawidłowo, użytkownik dokonuje wyboru aplikacji, w której zamierza pracować.

§21.

Obowiązkiem każdego pracownika jest dbałość o nie pozostawianie stanowiska informatycznego z dostępem do systemów bazodanowych, bez należytego zabezpieczenia , w tym:

1. opuszczając stanowisko pracy należy wylogować się z systemu,
2. przy krótkotrwałych przerwach w pracy należy zablokować stację roboczą.

§22.

Kończąc pracę w systemie użytkownik zamyka wszystkie otwarte aplikacje, a następnie zamyka system.

V. Środki ochrony systemu przed złośliwym oprogramowaniem, w tym wirusami komputerowymi

§23.

1. Za ochronę antywirusową odpowiada Administrator Systemu Informatycznego.
2. Czynności związane z ochroną antywirusową systemu informatycznego wykonuje ASI, wykorzystując w trakcie pracy systemu informatycznego moduł programu antywirusowego w aktualnej wersji, sprawdzającego na bieżąco zasoby systemu informatycznego.
3. Użytkownik systemu na stanowisku komputerowym, importujący dane osobowe do systemu informatycznego jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości występowania wirusów.
4 O wykryciu wirusa na stacji roboczej użytkownik powiadamia ASI.

5. ASI o przypadku stwierdzenia szczególnie groźnych lub trudnych do usunięcia wirusów komputerowych powiadamia Administratora Bezpieczeństwa Informacji.

§24.

Po dokonanej naprawie lub konserwacji należy przeprowadzić proces sprawdzenia pod kątem występowania wirusów.

§25.

Informatyczne nośniki informacji pochodzenia zewnętrznego podlegają sprawdzeniu programem antywirusowym przed rozpoczęciem korzystania z nich.

§26.

1. Nadzór nad prawidłowym funkcjonowaniem oprogramowania antywirusowego sprawuje Administrator Systemu Informatycznego.
2. ASI zobowiązany jest do przeprowadzania cyklicznej kontroli antywirusowej na wszystkich stanowiskach komputerowych.

§27.

1. Administrator Systemu Informatycznego jest odpowiedzialny za aktywowanie i poprawne konfigurowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku:

   a) sieci lokalnej i sieci rozległej,

   b) stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.

2. Użytkownicy systemu obowiązani są do utrzymywania stałej aktywności zainstalowanego na ich stanowiskach komputerowych specjalistycznego oprogramowania monitorującego wymianę danych na styku tego stanowiska i sieci lokalnej.

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

§28.

1. Aplikacje wykorzystywane do obsługi baz danych osobowych powinny zapewniać odnotowanie informacji o udzielonych odbiorcom danych.

2. Odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:

   a) osoby, której dane dotyczą,

   b) osoby użytkownika systemu lub innej osoby upoważnionej do przetwarzania danych osobowych w Urzędzie ,

   c) przedstawiciela, o którym mowa w art. 31a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,

   d) podmiotu, któremu powierzono przetwarzanie danych,

   e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

3. Odnotowanie powinno obejmować informacje o:

   a) nazwie jednostki organizacyjnej lub imieniu i nazwisku osoby, której udostępniono dane,

   b) zakresie udostępnianych danych,

   c) dacie udostępnienia,

4. Obowiązek odnotowania ww. informacji spoczywa na użytkowniku systemu, w tym celu wypełnia on odpowiednie pole w bazie danych osobowych.

5. Odnotowanie informacji powinno nastąpić niezwłocznie po udostępnieniu danych.

6. Udostępnienie danych osobowych może nastąpić wyłącznie na pisemną prośbę odbiorcy danych.

7. Na żądanie osoby, której dane zostały udostępnione, informacje o udostępnieniu danych są zamieszczane w raporcie z systemu informatycznego, a raport przekazywany tej osobie.

8. Nadzór nad prawidłowością odnotowywania w systemie ww. informacji sprawuje Administrator Systemu Informatycznego.

§29.

Pracownik, który udostępnia dane osobowe przetwarzane w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych, ma obowiązek prowadzenia rejestru udostępnionych danych, który musi zawierać co najmniej: datę udostępnienia, podstawę, zakres udostępnionych informacji oraz osobę lub instytucję dla której dane udostępniono.

VII. Procedury tworzenia kopii zapasowych

§30.

1 Administrator Systemu Informatycznego wykonuje regularnie kopie zapasowe danych przetwarzanych w systemie.
2 Kopie wykonywane są przy pomocy wbudowanych w system funkcji.
3 Kopie wykonywane są na macierze dyskowe znajdujące się w serwerowni .

VIII. Ogólne zasady i odpowiedzialność przy instalacji oprogramowania

§31.

1. Do instalacji i modyfikacji oprogramowania na serwerze uprawniony jest wyłącznie Administrator Systemu Informatycznego.

§32.

1. Instalowanie oprogramowania testowego i bezpłatnego dopuszcza się pod warunkiem otrzymania zgody na instalację od Administratora Danych,
2. O instalacji powiadamia się Administratora Bezpieczeństwa Informacji.

§33.

1. Administrator Systemu Informatycznego prowadzi wykaz oprogramowania dopuszczonego do używania w Urzędzie, którego wzór stanowi załącznik nr 5 do niniejszej instrukcji.
2. Kontroli podlega rodzaj oprogramowania oraz ilość licencji zakupionych przez Urząd.

§34.

Instalację lub modyfikację oprogramowania na serwerze lub stacji roboczej odnotowuje się na liście oprogramowania instalowanego.

§35.

Na wszystkich komputerach w Urzędzie dopuszcza się instalację tylko legalnego, licencjonowanego oprogramowania.

§36.

Wprowadza się następujące zasady korzystania z oprogramowania:

1. Oryginalne dokumenty licencyjne oraz nośniki każdego oprogramowania przechowywane są przez administratora systemu w zamkniętej szafie. Nośniki oprogramowania nie mogą znajdować się w żadnym innym miejscu, a szczególnie nie mogą być kopiowane, wypożyczane lub w żaden sposób przekazywane osobom trzecim. Dotyczy to również kodów aktywacyjnych produktów.
2. Zabrania się użytkownikom wykonywania kopii oprogramowania.
3. Wszyscy pracownicy zobowiązani są do pracy na legalnym oprogramowaniu oraz otrzymują wyraźny zakaz instalacji i użytkowania oprogramowania pochodzącego z innych źródeł.
4. Do podstawowych obowiązków pracownika należy korzystanie z oprogramowania w związku z wykonywaniem obowiązków pracowniczych, zgodnie z obowiązującymi przepisami prawa oraz wyłącznie w celach wykonywania obowiązków pracowniczych. Zabrania się korzystania z jakiegokolwiek oprogramowania do którego urząd nie jest uprawniony, w czasie pracy, w miejscu pracy ani przy użyciu sprzętu należącego do urzędu.

IX. Procedura i okres przechowywania nośników informacji, w tym kopii elektronicznych i wydruków.

§37.

1. Nośniki informacji, w tym kopie elektroniczne i wydruki zawierające dane nie mogą być dostępne dla osób nieuprawnionych.
2. Dane z magnetycznych nośników informacji usuwa się bezzwłocznie po ich wykorzystaniu służbowym, w sposób trwały.
3. Zabrania się sporządzania kopii baz danych na dyskach twardych stacji roboczych lub w folderach ogólnodostępnych w systemach Urzędu.

§38.

1. Użytkownik dokonujący wydruku na drukarce sieciowej, zobowiązany jest udać się niezwłocznie do pomieszczenia usytuowania drukarki i przejąć drukowany dokument.
2. Kopie błędne, nadmiarowe czy z innych powodów niepotrzebne należy niezwłocznie zniszczyć.
3. Wydruki, które nie podlegają archiwizacji należy niezwłocznie zniszczyć.
4. Każdy pracownik, który napotka wydruk, nośnik elektroniczny, czy inny dokument pozostawiony bez dozoru jest zobowiązany zabezpieczyć go i przekazać Administratorowi Bezpieczeństwa Informacji.

X. Procedura i harmonogram dokonywania przeglądów i konserwacji systemu oraz zbiorów danych.

§39.

Przeglądu i konserwacji systemu dokonuje w terminach określonych przez producenta sprzętu.

§40.

1. Przegląd systemu polega na sprawdzeniu jego konfiguracji oraz sprawdzeniu logów systemowych, ze szczególnym uwzględnieniem logów bezpieczeństwa.
2. W przypadku stwierdzenia nieprawidłowości w systemie, administrator systemu usuwa je,

wykorzystując dostępne narzędzia i odnotowuje ten fakt w dzienniku pracy serwera.
3. Jeżeli stwierdzone nieprawidłowości wskazują na działanie osób nieuprawnionych w systemie, administrator systemu podejmuje czynności zgodnie z zapisami „Polityki bezpieczeństwa Danych Osobowych w Urzędzie".

§41.

1. Konserwacja baz danych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów.
2. Przegląd zbiorów danych polega na:
   1) sprawdzeniu dostępu do zbiorów danych na poziomie użytkowników o różnych prawach dostępu,
   2) ocenie stanu zbiorów danych,
   3) sprawdzeniu ustawień dostępu dla poszczególnych użytkowników.
2. Administrator Systemu zobowiązany jest uaktywnić mechanizm zliczania nieudanych prób zalogowania się do systemu oraz ustawić blokadę konta użytkownika po wykryciu trzech nieudanych prób, we wszystkich systemach posiadających taką funkcję.
3. W przypadku stwierdzenia nieprawidłowości w stanie zbiorów danych lub naruszenia praw dostępu, administrator systemu powiadamia o zaistniałym fakcie Administratora Bezpieczeństwa Informacji, a następnie podejmuje działania zmierzające do usunięcia nieprawidłowości i zidentyfikowania osoby, która doprowadziła do ich powstania.
4. W przypadku wykrycia użytkowników nieuprawnionych, których działania mogły doprowadzić do: przeglądania, przenikania, wnioskowania, zniekształcania, powtarzania, wstawiania, niszczenia, kradzieży, modyfikacji, szpiegostwa, blokowania usług systemu, itp., administrator systemu podejmuje czynności zgodnie z zapisami rozdziału VIII „Polityki Przetwarzania Danych Osobowych w Urzędzie Gminy Słupno".

XI. Zasady wyposażania i eksploatacji stacji roboczych

§42.

1. Administrator systemu nadzoruje proces zakupu sprzętu komputerowego oraz oprogramowania.
2. Instalacja sprzętu komputerowego na stanowiskach pracy wykonywana jest przez administratora systemu lub pracowników firmy której powierzono serwis systemu.
3. Przeniesienia sprzętu do innych pomieszczeń wykonywane będą przez administratora systemu bądź pracowników firmy, której powierzono serwis systemu. Zabrania się samodzielnego przenoszenia sprzętu przez innych pracowników.
4. Użytkownicy ponoszą odpowiedzialność materialną za powierzony im sprzęt komputerowy.

XII. Procedura zarządzania sprzętem komputerowym.

§43.

1. Procedura zgłaszania zapotrzebowania na sprzęt komputerowy:
   1) zgłoszenie ASI zapotrzebowania na sprzęt komputerowy poprzez wypełnienie formularza zapotrzebowania stanowiący Załącznik Nr 3 do Instrukcji Zarządzania Systemem Komputerowym, ASI konsultuje zgłoszenie z Skarbnikiem oraz Sekretarzem Gminy,
   2) decyzje o zakupie oraz o trybie zakupu podejmuje Wójt,

§44.

Procedura zakupu sprzętu komputerowego.

1. Na początku roku kalendarzowego, po przyjęciu budżetu, ASI wraz ze Skarbnikiem oraz Sekretarzem Gminy decydują o strategii zakupów inwestycyjnych i podejmowane są decyzje o kolejności zakupów.
2. Zakupy sprzętu komputerowego dokonywane są w oparciu o ustawę o zamówieniach publicznych,
3. ASI przygotowuje Specyfikacje Istotnych Warunków Zamówienia, która jest zatwierdzana przez Wójta,
4. Rozstrzygnięcie postępowania przetargowego regulują odrębne przepisy,

5. W sytuacjach awaryjnych (nagła awaria sprzętu, itp.) procedura przewiduje zakupy z wolnej ręki.

§45.

Procedura przyjęcia do ewidencji sprzętu komputerowego.

1. Każdorazowo po zakupie sprzętu komputerowego ASI wprowadza jego parametry do Ewidencji Środków Trwałych części teleinformatycznej którą stanowi Załącznik nr 2 do Instrukcji Zarządzania Sprzętem Komputerowym, prowadzonej w sposób elektroniczny i nadaje mu numer inwentarzowy,
2. ASI wypełnia zgłoszenie sprzętu komputerowego do Referatu Planowania i Finansów prowadzącego Ewidencję Środków Trwałych Urzędu Gminy Słupno.
3. Referat Finansowy wprowadza do Ewidencji Środków Trwałych zakupiony sprzęt komputerowy.

§46.

Procedura instalacji sprzętu komputerowego na stanowisku pracy.

1. Przed instalacją sprzętu komputerowego na stanowisku pracy ASI sprawdza działanie urządzeń, aby w razie problemów zgłosić reklamacje,
2. Po zainstalowaniu sprzętu komputerowego na stanowisku pracy ASI dokonuje instruktarzu pracownika i zapoznaje z ewentualnymi nowymi funkcjami urządzeń i programów zainstalowanych na komputerze.

§47.

Procedura zmiany lokalizacji/ osoby użytkującej sprzęt komputerowy

1. W razie zmiany lokalizacji, zmiany osoby użytkującej sprzęt komputerowy ASI aktualizuje wszystkie rejestry i ewidencje dotyczące tego pracownika i sprzętu komputerowego,
2. O zmianie osoby przypisanej do sprzętu komputerowego bądź lokalizacji urządzeń ASI dokonuje aktualizacji w Załączniku Nr 2 Instrukcji Zarządzania Sprzętem Komputerowym, oraz przekazuję tą zmianę do Referatu Planowania i Finansów.

§58.

Procedura likwidacji sprzętu komputerowego.

1. Jeśli sprzęt komputerowy:
   a) jest uszkodzony i jego naprawa jest nieopłacalna lub niemożliwa,
   b) jest przestarzały i niespełna wymagań technicznych zainstalowanego oprogramowania w urzędzie,
   c) został uszkodzony, a zakup nowego podzespołu naruszałby umowę licencyjną oprogramowania dołączoną do tego sprzętu; to zostaje on poddany Procedurze likwidacji.
2. Sprzęt komputerowy do likwidacji typuje ASI i w porozumieniu z Sekretarzem Gminy lub Wójtem i przygotowuje Wniosek typowania sprzętu komputerowego do likwidacji, stanowiący załącznik Nr 4 do Instrukcji Zarządzania Sprzętem Komputerowym
3. Na podstawie Wniosku sprzęt zostaje przekazany do utylizacji odpowiednio wyspecjalizowanej firmie.
4. Firma sporządza Protokół likwidacji sprzętu komputerowego w dwóch egzemplarzach dla Referatu Planowania i Finansów i ASI.
5. Referatu Planowania i Finansów wykreśla z Ewidencji Środków Trwałych zlikwidowany sprzęt komputerowy, także ASI zaznacza w swojej Ewidencji, że dane urządzenie zostało zlikwidowane.

§49.

Procedura utylizacji sprzętu komputerowego.

1. Po zgromadzeniu odpowiedniej ilości zepsutego sprzętu komputerowego zostaje on poddany procedurze utylizacji.
2. W wyniku wewnętrznych konsultacji zostaje wyłoniona firma utylizacyjna.
3. ASI przekazuje firmie utylizacyjnej popsuty sprzęt komputerowy a następnie sporządzany zostaje w dwóch egzemplarzach protokół przekazania sprzętu komputerowego do utylizacji.
4. Firma utylizacyjna jest zobowiązana do przekazania Urzędowi Protokołu utylizacji sprzętu komputerowego.
5. Referat Planowanie i Finansów zdejmuję sprzęt komputerowy ze stanu urzędu na podstawie protokołu utylizacji.

§50.

W określonych przypadkach zachodzi możliwość przekazania sprzętu komputerowego podmiotowi zewnętrznemu.

§51.

Procedura konserwacji i rozbudowy sprzętu komputerowego.

1 ASI dokonuje okresowej konserwacji sprzętu komputerowego.
2 Jeżeli procedura konserwacji nie przeszkadza w znaczący sposób w funkcjonowaniu Urzędu może ona być dokonywana w godzinach pracy, w przeciwnym wypadku po zakończeniu pracy Urzędu.
3 ASI dokonuje rozbudowy/ modernizacji sprzętu komputerowego zgodnie z zasadami bezpieczeństwa BHP oraz zgodnie z przepisami licencyjnymi oprogramowania zainstalowanego na rozbudowywanym/modernizowanym komputerze.

XIII. Postanowienia końcowe

§52.

Przestrzeganie postanowień niniejszej Instrukcji przez użytkowników systemów stanowi podstawę bezpiecznego posługiwania się systemami Urzędu.

§53.

Instrukcja nie może być wynoszona z obiektów Urzędu, powielana w części lub całości bez zgody Administratora Bezpieczeństwa Informacji.

§54.

1. Postanowienia niniejszej Instrukcji mogą być modyfikowane zarządzeniem Wójta wraz ze zmianami w systemach informatycznych Urzędu.
2. Propozycje zmian może składać pisemnie każdy pracownik Urzędu korzystając z drogi służbowej lub bezpośrednio do Administratora Bezpieczeństwa Informacji.

§55.

Administrator Bezpieczeństwa Informacji okresowo monitoruje przestrzeganie przez pracowników Urzędu zasad i przepisów ochrony danych osobowych.

§56.

W kwestiach nie uregulowanych niniejszą Instrukcją mają zastosowanie unormowania Regulaminu Pracy Urzędu, przepisy Kodeksu Pracy i Ustawy o ochronie danych osobowych wraz z aktami wykonawczymi.

Załącznik nr 1
do Instrukcji Zarządzania
Systemem Informatycznym
w Urzędzie Gminy Słupno

Słupno, dnia .....r.

Zapotrzebowanie na oprogramowanie komputerowe

Imię i nazwisko: .....

Referat: .....

Zgłasza zapotrzebowanie na oprogramowanie komputerowe.

1. Opis zapotrzebowania

Rodzaj lub nazwa oprogramowania komputerowego	**X**
Edytor tekstu	
Arkusz kalkulacyjny	
Program do tworzenia prezentacji	
Program graficzny	
Podpis elektroniczny	
Inne:	

2. Opis przeznaczenia programu:
.....
.....
.....

.....
Podpis pracownika

Załącznik nr 2
do Instrukcji Zarządzania Systemem Informatycznym
w Urzędzie Gminy Słupno

Ewidencja Środków Trwałych

Lp.	Data przychodu/ rozchodu	Numer inwentarzowy	Nazwa przedmiotu, opis i stan	Naprawy/ wymiany	Miejsce przeznaczenia/ użytkowania	Cena jedn.
1	2	3	4	5	6	
1.						

Załącznik nr 3
do Instrukcji Zarządzania
Systemem Informatycznym
w Urzędzie Gminy Słupno

Słupno, dnia .....r.

Zapotrzebowanie na sprzęt komputerowy

Imię i nazwisko: .....

Wydział: .....

Zgłasza zapotrzebowanie na sprzęt komputerowy.

1. Opis zapotrzebowania.

Rodzaj sprzętu	X
Jednostka Centralna	
Monitor	
Drukarka	
Skaner	
Klawiatura	
Mysz	
Nagrywarka	
UPS	
Dysk Twardy	
Czytnik Kart Pamięci	
Inne:	

2. Przyczyna zapotrzebowania na nowy sprzęt komputerowy:

.....

.....

.....

.....

.....
Podpis pracownika

Załącznik nr 4
do Instrukcji Zarządzania
Systemem Informatycznym
w Urzędzie Gminy Słupno

Słupno, dnia .....r.

Urząd Gminy w Słupnie
ul. Miszewska 8A
09-472 Słupno

Wniosek typowania do likwidacji sprzętu komputerowego

W dniu ..... skierowano do likwidacji następujący sprzęt komputerowy:

Lp.	Rodzaj sprzętu	Numer inwentarzowy	Miejsce użytkowania	Powód wytypowania do likwidacji
1.				
2.				

.....
Przyjmujący do utylizacji

.....
Administrator Systemów Informatycznych

Załącznik nr 5 do
do Instrukcji Zarządzania Systemem Informatycznym
w Urzędzie Gminy Słupno

EWIDENCJA OPROGRAMOWANIA W URZĘDZIE GMINY SŁUPNO

Lp.	Nazwa programu	Numer licencyjny	Data instalacji	Numer komputera	Nazwisko i imię osoby pracującej na komputerze	Nazwisko i imię osoby instalującej

.....
(podpis Administratora Danych Osobowych)