BURMISTRZ
Miasta i Gminy Kunów

Zarządzenie Nr 59/15
Burmistrza Miasta i Gminy Kunów
z dnia 11.03.2015 r.

w sprawie: wdrożenia Instrukcji Zarządzania Systemem Informatycznym Urzędu Miasta i Gminy w Kunowie.

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. z 2014 r. poz. 1182 z późn. zm.) oraz § 3 i § 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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 2004r. Nr 100, poz. 1024) – zarządzam co następuje:

§ 1.

Wprowadza się do użytku służbowego **Instrukcję Zarządzania Systemem Informatycznym** w brzmieniu stanowiącym załącznik Nr 1 do niniejszego zarządzenia.

§ 2.

Instrukcja ma zastosowanie na wszystkich stanowiskach pracy, gdzie przetwarzane są dane osobowe lub praca odbywa się w systemie informatycznym Urzędu Miasta i Gminy w Kunowie.

§ 3.

1. Zobowiązuje się wszystkich pracowników Urzędu Miasta i Gminy w Kunowie, do zapoznania się z treścią **Instrukcji**, w terminie dwóch tygodni od dnia wejścia w życie Zarządzenia oraz praktycznego wdrożenia określonych w niej zasad przetwarzania danych osobowych i bezpiecznej pracy w systemie informatycznym Urzędu.
2. Za wykonanie postanowień ust. 1 odpowiadają bezpośredni przełożeni.

§ 4.

Wykonanie Zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 5.

Zarządzenie wchodzi w życie z dniem podjęcia.

BURMISTRZ
mgr Lech Łodej

BURMISTRZ
Miasta i Gminy Kunów

Załącznik Nr 1
do Zarządzenia Nr 59/15
Burmistrza Miasta i Gminy w Kunowie
z dnia 11.03.2015 r

Zatwierdzam

.....

Burmistrz Miasta i Gminy Kunów

Instrukcja Zarządzania Systemem Informatycznym Urzędu Miasta i Gminy w Kunowie

I. Wstęp

Podstawę prawną dla opracowania i wdrożenia niniejszej instrukcji stanowią: Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity: Dz.U. z 2014 r. poz. 1182 z późn. zm.) oraz Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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.).

II. Przepisy ogólne

1. **Instrukcja zarządzania systemem informatycznym Urzędu Miasta i Gminy w Kunowie**, zwana dalej **Instrukcją**, opisuje sposoby nadawania uprawnień użytkownikom, określa sposób pracy w systemie informatycznym, procedury zarządzania oraz czynności mające wpływ na zapewnienie bezpieczeństwa systemu informatycznego.
2. Niniejsza **Instrukcja** realizuje **Politykę Bezpieczeństwa Przetwarzania Danych Osobowych** obowiązującą w Urzędzie Miasta i Gminy w Kunowie.

III. Definicje

ekroć w niniejszym dokumencie jest mowa o:

- **Urzędzie** – należy przez to rozumieć Urząd Miasta i Gminy w Kunowie,
- Administratorze Danych Osobowych (**ADO**) - należy przez to rozumieć Burmistrza Miasta i Gminy Kunów,
- Administratorze Bezpieczeństwa Informacji (**ABI**) – należy przez to rozumieć wyznaczonego Zarządzeniem Burmistrza pracownika do nadzorowania przestrzegania przepisów o ochronie danych osobowych i prowadzenia rejestru zbiorów danych osobowych przetwarzanych w **Urzędzie,**
- Administratorze Systemu Informatycznego (**ASI**) – należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemu informatycznego urzędu oraz stosowanie technicznych i organizacyjnych środków ochrony,

- Systemie informatycznym, zwanym dalej **Systemem** – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
- Użytkowniku systemu – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym urzędu,
- Ustawie – należy rozumieć Ustawę z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity: Dz.U. z 2014 r. poz. 1182 z późn. zm.)
- Rozporządzeniu – należy rozumieć Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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.).
- Sieci lokalnej – należy przez to rozumieć fizyczne i logiczne połączenie systemów informatycznych urzędu z wykorzystaniem urządzeń telekomunikacyjnych,
- Sieci Internet – należy przez to rozumieć publiczną sieć telekomunikacyjną w rozumieniu Ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (tekst jednolity: Dz. U. z 2014r., poz. 243 z późn. Zm.)

IV. Poziom bezpieczeństwa

W **Urzędzie** obowiązuje wysoki poziom bezpieczeństwa systemu informatycznego z uwagi na to, że jest on połączony z siecią publiczną (z Internetem)

7. Bezpieczna eksploatacja sprzętu i oprogramowania

Celem procedury jest określenie wymagań bezpieczeństwa sprzętu i oprogramowania eksploatowanego w **Urzędzie**.

1. W celu zagwarantowania spójności przetwarzanych danych każda stacja robocza korzysta ze specjalnie dla tego celu wydzielonej sieci zasilającej, podłączonej do urządzenia UPS zabezpieczającego sieć na ewentualność zaników napięcia w sieci energetycznej.
2. Urządzenia aktywne obsługujące sieć lokalną **Urzędu** chronią ją na poziomie warstwy łącza danych na ewentualność podłączenia obcych urządzeń.
3. Ekrany monitorów są wyposażone w wygaszacze zabezpieczone hasłem, które aktywują się automatycznie po upływie określonego czasu od ostatniego użycia komputera.

4. Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych są użytkowane z zachowaniem praw autorskich i posiadają licencje.
5. Instalacji oprogramowania może dokonywać tylko **ASI**. W razie konieczności instalacji oprogramowania przez pracowników firm zewnętrznych czynność ta powinna być wykonywana za przyzwoleniem i w obecności **ASI**.
6. **System** wyposażony jest w mechanizmy autoryzacji oraz uwierzytelniania użytkownika sprawujące kontrolę dostępu do danych osobowych jedynie osób upoważnionych.
7. Użytkownikom nie wolno uruchamiać oprogramowania z innych źródeł (nośniki wymienne, Internet) bez zgody **ASI.**
8. Komputer przenośny może być używany do przetwarzania danych osobowych po odpowiednim jego zabezpieczeniu.
9. Użytkownik korzystający z komputera przenośnego jest zobowiązany do zachowania szczególnej ostrożności podczas transportu komputera oraz nie może udostępnić komputera osobom nieupoważnionym.
10. Ekrany monitorów są ustawiane w miarę możliwości w taki sposób, żeby uniemożliwić odczyt wyświetlanych informacji osobom nieupoważnionym.
11. Za spełnienie obowiązków określonych w punkcie 2-6 powyższego rozdziału instrukcji odpowiada **ASI.**
12. Za spełnienie obowiązków określonych w punkcie 7-10 powyższego rozdziału instrukcji odpowiadają użytkownicy korzystający z komputera

VI. Procedura korzystania z Internetu i poczty elektronicznej.

Celem procedury jest uregulowanie zasad korzystania z Internetu i poczty elektronicznej, aby zagwarantować bezpieczeństwo danych osobowych przesyłanych przez te media.

Użytkownicy Internetu zobowiązani są do przestrzegania następujących zasad:

a. Zakazuje się ściągania przez użytkowników plików lub przeglądania zasobów informacyjnych o treści prawne zabronionej, obscenicznej bądź pornograficznej.
b. Zaleca się, aby do wymiany korespondencji w czasie korzystania z **Systemu Urzędu** wykorzystywać jedynie służbową pocztę elektroniczną.
c. Szczególne rygory należy stosować wobec ściągania z Internetu plików wykonywalnych. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowania ściągnięte z Internetu i przez niego używane.

d. Do korzystania z Internetu użytkownicy mogą wykorzystywać jedynie zaakceptowane przez **ASI** formy dostępu (dotyczy prób obchodzenia poustawianych obostrzeń oraz podłączania dodatkowych urządzeń komunikacyjnych).

Użytkownicy systemu poczty elektronicznej zobowiązani są do przestrzegania następujących zasad:

1. Przesyłanie informacji za pośrednictwem poczty elektronicznej winno odbywać się zgodnie z uprawnieniami adresatów do korzystania z określonego typu danych. W przypadku wątpliwości nadawca powinien sprawdzić, czy dana osoba ma uprawnienia do korzystania z dokumentów danego typu lub o określonej klauzuli poprzez skonsultowanie się z **ABI**.
2. Jeśli adresatem wiadomości zawierającej dane osobowe jest pracownik **Urzędu** zaleca się doręczenia danych w formie elektronicznej w sposób wykorzystujący wewnętrzne mechanizmy przekazywania danych (dyski sieciowe, udostępniony folder użytkownika docelowego).
3. Przesyłanie informacji poza obręb **Urzędu** może odbywać się tylko przez osoby do tego upoważnione do adresatów upoważnionych do przesyłanych danych.
4. W razie konieczności przesyłania danych osobowych dane te należy uprzednio odpowiednio zabezpieczyć wykorzystując mechanizmy kompresji z szyfrowaniem z tym zastrzeżeniem, że hasło musi zostać dostarczone do adresata droga inną niż same dane (np. przez telefon) Złożoność hasła: na poziomie min. 8 znaków w tym duża, mała litera, znak specjalny oraz cyfra.
5. Użytkownicy powinni zwrócić szczególną uwagę na poprawność adresu odbiorcy dokumentu.
6. Jeżeli istotne jest potwierdzenie otrzymania przez adresata przesyłki, użytkownik winien skorzystać z opcji systemu poczty elektronicznej informującej o dostarczeniu i otwarciu dokumentu. Dodatkowo zaleca się, aby użytkownik zawarł w treści dokumentu prośbę o potwierdzenie otrzymania i zapoznania się z informacją.
7. Informacje przesyłane za pośrednictwem poczty elektronicznej muszą być zgodne z prawem i zasadami zawartymi w **Polityce Bezpieczeństwa Przetwarzania Danych Osobowych** obowiązującej w **Urzędzie**.
8. Użytkownicy nie powinni otwierać przesyłek od nieznanych sobie osób, których tytuł nie sugeruje związku z wypełnianymi przez nich obowiązkami służbowymi. W przypadku

otrzymania takiej przesyłki, użytkownik powinien ją zniszczyć lub skontaktować się z **ASI.**

9. Użytkownicy nie powinni uruchamiać wykonywalnych załączników (pliki.exe) dołączonych do wiadomości przesyłanych pocztą elektroniczną. W takim przypadku użytkownik powinien poinformować o zdarzeniu **ASI**, który winien sprawdzić czy załącznik stanowi zagrożenie dla przetwarzanych w **Systemie** informacji.
10. Użytkownicy nie powinni rozsyłać za pośrednictwem poczty elektronicznej informacji o zagrożeniach systemu informatycznego, łańcuszków szczęścia itp.
11. Użytkownicy nie powinni rozsyłać, wiadomości o dużym rozmiarze do większej liczby adresatów. W razie konieczności przesłania większych załączników winni skontaktować się z **ASI.**
12. Użytkownicy powinni okresowo kasować niepotrzebne wiadomości pocztowe.

VII. Procedura nadawania i zmiany uprawnień do przetwarzania danych osobowych

Celem procedury jest zapewnienie użytkownikom odpowiednich uprawnień do przetwarzania danych osobowych, aby redukować zagrożenie nieuprawnionego dostępu do danych osobowych i utraty poufności.

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:
   - ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. z 2014 r. poz. 1182 z późn. Zm.),
   - **Polityką Bezpieczeństwa Przetwarzania Danych Osobowych** w Urzędzie Miasta i Gminy w Kunowie
   - niniejszym dokumentem,

   oraz posiadać upoważnienie do przetwarzania danych osobowych.
2. Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór przedstawia **Załącznik nr 1.**
3. **ASI** przyznaje uprawnienia z zakresie dostępu do **Systemu** na podstawie wniosku złożonego przez bezpośredniego przełożonego pracownika, którego wniosek dotyczy. Wniosek musi zaakceptowany przez **ABI** – wzór wniosku przedstawia **Załącznik nr 2.**

4. Przyznanie uprawnień w zakresie dostępu do **Systemu** polega na wprowadzeniu do niego dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakres dostępu danych i operacji.
5. Hasło ustanowione podczas przyznawania uprawnień przez **ASI** należy zmienić na indywidualne podczas pierwszego logowania się w **Systemie.**
6. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony – wzór upoważnienia przedstawia **Załącznik nr 3.**
7. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
8. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie wyrejestrować z **Systemu**, w którym są one przetwarzane oraz unieważnić jej hasło
9. W **Systemie** stosuje się uwierzytelnianie dwustopniowe na poziomie dostępu do systemu operacyjnego i sieci lokalnej oraz dostępu do aplikacji.
10. Odebranie uprawnień pracownikowi następuje na pisemny wniosek bezpośredniego przełożonego, **ABI** lub **ADO** z podaniem daty oraz przyczyny odebrania uprawnień.
11. **ADO** jest zobowiązany poinformować **ABI** o każdej zmianie dotyczącej pracowników mogącej mieć wpływ na zakres posiadanych przez nich uprawnień w systemie informatycznym.
12. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie wyrejestrować z **Systemu**, w którym są one przetwarzane oraz unieważnić jej hasło.
13. **ASI** zobowiązany jest do prowadzenia i ochrony **Rejestru użytkowników i ich uprawnień w systemie informatycznym**, który przedstawia **Załącznik nr 4.**

VIII. Metody i środki uwierzytelnienia

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane osobowe maja dostęp jedynie osoby do tego upoważnione.

1. Bezpośredni dostęp do **Systemu** można mieć wyłącznie po podaniu identyfikatora osoby i właściwego hasła.
2. Pierwsze hasło dla użytkownika ustala **ASI** przy wprowadzaniu identyfikatora użytkownika do **Systemu.**

3. Użytkownik **Systemu** niezwłocznie ustala swoje, znane tylko jemu hasło, po nadaniu hasła przez **ASI.**
4. Użytkownik **Systemu** w trakcie pracy w aplikacji może zmienić swoje hasło dostępu.
5. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numeru PESEL, numerów telefonów itp.
6. Hasło nie może być ujawnione nawet po utracie przez nie ważności.
7. Hasła maja charakter poufny – są znane tylko jego właścicielowi.
8. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.
9. Hasło winno składać się co najmniej z 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne o ile system informatyczny i oprogramowanie na to pozwala.
10. O ile aplikacja nie umożliwia wymuszania zasad zmiany haseł za systematyczną oraz terminowa zmianę hasła odpowiada użytkownik.
11. Zmiana hasła do systemu operacyjnego następuje nie rzadziej, niż co 30 dni .
12. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła i poinformowania o zaistniałym fakcie **ABI.**
13. Hasła administratora do poszczególnych programów / systemów powinny być spisane oraz umieszczone w zamkniętej kopercie w miejscu uniemożliwiającym dostęp do nich osób nieupoważnionych, chroniącym przed utratą lub zniszczeniem oraz gwarantującym ich odczytanie upoważnionemu użytkownikowi, a także kierownikowi urzędu.
14. Zarejestrowane hasła administratora, oprócz treści hasła winny posiadać adnotację o dacie ich wprowadzenia do **Systemu.**
15. W przypadku utraty uprawnień przez osobę administrującą **Systemem** należy niezwłocznie zmienić hasła, do których miała dostęp.
16. Identyfikator użytkownika nie może być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z **Systemu** nie może zostać przydzielany innej osobie.
17. Pracownicy są odpowiedzialni za zachowanie poufałości swoich identyfikatorów

IX. Procedura rozpoczęcia, zawieszenia i zakończenia pracy w systemie

Celem procedury jest zabezpieczenie danych osobowych przed nieuprawnionym dostępem i utrata poufności w sytuacji gdy użytkownik rozpoczyna, przerywa lub kończy pracę w **Systemie** przetwarzającym dane osobowe.

1. Rozpoczynając pracę na komputerze użytkownik loguje się do **Systemu**.
2. Dostęp do danych osobowych możliwy jest jedynie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia użytkownika.
3. Jeżeli **System** to umożliwia **ASI** zobowiązany jest uaktywnić mechanizm zaliczania nieudanych prób dostępu do **Systemu** oraz ustawić blokadę konta na poziomie danego użytkownika po wykryciu trzech nieudanych prób logowania.
4. **ASI** ustala przyczyny zablokowania **Systemu** oraz w zależności od zaistniałej sytuacji podejmuje odpowiednie działania. O zaistniałym incydencie powiadamia **ABI**.
5. Przed opuszczeniem stanowiska pracy, użytkownik obowiązany jest:
   a) wylogować się z **Systemu** lub,
   b) wywołać blokowany hasłem wygaszacz ekranu.
6. Kończąc pracę należy:
   a) wylogować się z **Systemu**, a następnie wyłączyć sprzęt komputerowy,
   b) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

X. Procedura tworzenia kopii zapasowych

Tworzenie kopii bezpieczeństwa danych osobowych z programów.

1. Za systematyczne przygotowanie kopii bezpieczeństwa i weryfikację ich poprawności odpowiada **ASI**.
2. Kopie zapasowe danych z programów przetwarzających dane osobowe wykonywane są na koniec każdego dnia roboczego z wykorzystaniem odpowiednio skonfigurowanych zasobów sieciowych **Urzędu**.
3. Kopie bezpieczeństwa na nośniku zewnętrznym wykonywane są w cyklu tygodniowym oraz miesięcznym, a także przed każdą aktualizacją programów.
4. Kopie bezpieczeństwa wykonywane są na płytach CD/DVD.
5. Zachowuje się minimum 12 kopii bezpieczeństwa z poprzednich miesięcy.
6. Dodatkowe zapasowe kopie bezpieczeństwa wszystkich programów i danych wykonywane są w pierwszym dniu każdego miesiąca w postaci zapisu na płytach DVD-R.

7. Poza nośnikiem zewnętrznym miesięczne kopie bezpieczeństwa przechowywane są na serwerach plików odpowiednio do tego zabezpieczonych.

XI. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz wydruków

Procedura określa sposób postępowania z nośnikami, na których znajdują się dane osobowe, celem zabezpieczenia ich przed niszczeniem, kradzieżą, dostępem osób nieupoważnionych.

1. **Elektroniczne nośniki informacji**
   - Pracownicy nie mogą wynosić na zewnątrz **Urzędu** wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody **ADO**.
   - Dane osobowe w postaci elektronicznej – za wyjątkiem kopii bezpieczeństwa – zapisane na różnych nośnikach pamięci np. płytach CD/DVD, pendrive, dyskietkach, przenośnych dyskach twardych nie mogą opuścić obszaru przetwarzania danych osobowych.
   - Elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych).
   - Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a następnie są one fizycznie niszczone w obecności **ABI** i **ASI**, co zostaje potwierdzone ich podpisami w **Rejestrze nośników komputerowych zawierających ważne dane** - wzór rejestru stanowi **załącznik nr 5**.
   - Elektroniczne nośniki informacji, zawierające dane osobowe, nie mogą zostać przekazane innemu podmiotowi nieuprawnionemu do dostępu do tych danych, nawet po uprzednim usunięciu danych z nośnika.
   - Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem **ASI**.
   - Zaleca się, aby informacje wewnętrzne znajdujące się na nośnikach przenośnych, wynoszonych poza teren **Urzędu**, były szyfrowane.

2. **Kopie zapasowe**

- Kopie bezpieczeństwa zbioru danych osobowych oraz oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych osobowych są przechowywane w ognioodpornym sejfie (metalowej szafie) ustawionym/ej w miejscu wskazanym przez **ABI** w budynku Urzędu Miasta i Gminy w Kunowie.
- Dostęp do wykonanych kopii bezpieczeństwa zbioru danych osobowych, oprogramowania i narzędzi programowych, o których mowa powyżej, ma **ASI , ABI** oraz **ADO.**
- Nośniki, na których znajdują się kopie zawierające dane osobowe, są oznaczone w sposób trwały, jednoznaczny i czytelny oraz zaewidencjonowane w **Rejestrze nośników komputerowych zawierających ważne dane** stanowiącym **Załącznik nr 5** do niniejszej Instrukcji.
- Kopie archiwalne należy okresowo sprawdzać pod kątem ich dalszej przydatności do odtwarzania oraz bezzwłocznie je usuwać po ustaniu ich użyteczności.

3. **Wydruki**
   - Wydruki zawierające dane osobowe przechowywane są w pokojach stanowiących obszar przetwarzania danych osobowych w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (typu: zalanie, pożar).
   - Pomieszczenia, w których przechowywane są wydruki robocze muszą być należycie zabezpieczone po godzinach pracy.
   - Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie, np. poprzez pocięcie w niszczarce.
   - Za bezpieczeństwo danych osobowych zapisanych w formie tradycyjnej odpowiedzialne są osoby je przetwarzające.

XII. Sposób zabezpieczenia systemu informatycznego przed wirusami i szkodliwym oprogramowaniem

- Za ochronę antywirusową odpowiada **ASI.**
- Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe z włączoną ochroną antywirusową i antyspyware.
- Programy antywirusowe, o których mowa poprzednio, winny być uaktywnione cały czas podczas pracy danego systemu.

- Definicje wzorców wirusów aktualizowane są codziennie.
- Wszystkie pliki otrzymywane z zewnątrz, jak również wysyłane na zewnątrz, podlegaja sprawdzeniu pod kątem występowania wirusów najnowszą dostępną wersja programu antywirusowego.
- Bezwzględnie zabrania się używania nośników niewiadomego pochodzenia.
- Bezwzględnie zabrania się pobierania z sieci Internet plików niewiadomego pochodzenia.
- **ASI** przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach – minimum co dwa miesiące.
- Kontrola antywirusowa przeprowadzona jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.
- W przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik winien powiadomić **ASI**.
- W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wirus wykryto oraz wszystkie posiadane przez użytkownika nośniki.

XIII. Zasady udostępnienia oraz przekazywania danych osobowych innym osobom i instytucjom

1. Zgodnie z art. 7 pkt. 6 Ustawy odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:
   a. osoby, której dane dotyczą,
   b. osoby upoważnionej do przetwarzania danych,
   c. przedstawiciela, o którym mowa w art. 31 Ustawy,
   d. podmiotu, o którym mowa w art.31 Ustawy,
   e. organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
2. Dane osobowe administrowane przez urząd udostępnia się osobom lub podmiotom uprawnionym do ich otrzymywania na mocy Ustawy oraz innych przepisów powszechnie obowiązujących.
3. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną.

4. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej.
5. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych oraz wskazać ich zakres i przeznaczenie – wzór wniosku określa **Załącznik nr 6.**
6. Dane udostępnione urzędowi przez inny podmiot można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
7. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym system ten zapewnia odnotowanie: :
   1) daty pierwszego wprowadzenia danych do sytemu,
   2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu,
   3) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą,
   4) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 Ustawy,
   5) sprzeciwu, o którym mowa w art. 32 ust.1 pkt 8 Ustawy.

   oraz sporządzenie i wydrukowanie raportu zawierającego ww. informacje dla każdej osoby, której dane są przetwarzane w systemie informatycznym.
8. Jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z ustawy o ochronie danych osobowych – stosuje się przepisy tych ustaw (np. ustawa z dnia 29 sierpnia 1997r. Ordynacja podatkowa).

XIV. Procedury wykonywania przeglądów i konserwacji systemu

1. Aktualizacja oprogramowania powinna być przeprowadzana zgodnie z zaleceniami producentów oraz opinia rynkową co do bezpieczeństwa stabilności nowych wersji.
2. Przeglądy i konserwacja urządzeń wchodzących w skład **Systemu** powinny być wykonywane w terminach określonych przez producenta sprzętu.
3. Za terminowość przeprowadzenia aktualizacji, przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada **ASI.**
4. Zauważone nieprawidłowości w działaniach **Systemu** oraz oprogramowania powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości **ASI** zawiadamia **ABI.**
5. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia **Systemu**, wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach

określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.

6. W przypadku naprawy sprzętu komputerowego dane osobowe należy zabezpieczyć, natomiast w przypadku naprawy sprzętu poza terenem **Urzędu,** po zabezpieczeniu danych, usunąć z dysku. Gdy nie ma możliwości usunięcia danych, naprawa powinna być nadzorowana przez **ASI.**
7. Działania konserwacyjne, awarie oraz naprawy są rejestrowane w **Dzienniku systemu informatycznego UMiG,** który prowadzi **ASI. Dziennik systemu informatycznego UMiG** przedstawia **Załącznik nr 7.**
8. Wpisów do dziennika mogą dokonywać **ADO, ABI** i **ASI.**

XV. Załączniki

1. **Załącznik nr 1** – Wzór – Oświadczenie pracownika Urzędu o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych;
2. **Załącznik nr 2** – Wzór – Wniosek o nadanie uprawnień w systemie informatycznym;
3. **Załącznik nr 3** – Wzór – Upoważnienie do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Kunowie;
4. **Załącznik nr 4** – Rejestr użytkowników i ich uprawnień w systemie informatycznym;
5. **Załącznik nr 5** – Rejestr nośników komputerowych zawierających ważne dane;
6. **Załącznik nr 6** – Wzór – Wniosek o udostępnienie danych ze zbioru danych osobowych;
7. **Załącznik nr 7** - Dziennik systemu informatycznego Urzędu Miasta i Gminy w Kunowie.

BURMISTRZ
mgr Lech Łodej

BURMISTRZ
Miasta i Gminy Kunów

Załącznik nr 1
do Instrukcji Zarządzania Systemem Informatycznym
w UMiG w Kunowie

.....
(imię i nazwisko pracownika)

.....
(stanowisko i nazwa komórki organizacyjnej Urzędu)

O Ś W I A D C Z E N I E

pracownika Urzędu o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych

Oświadczam, że zapoznałam(em) się z przepisami dotyczącymi ochrony danych osobowych i zobowiązuję się do przestrzegania:

1. **Ustawy z dnia 29 sierpnia 1997r.** o ochronie danych osobowych (tekst jednolity: Dz.U. z 2014 r. poz. 1182 z późn. zm.).
2. **Rozporządzenia Ministra Spraw Wewnętrznych i Administracji** z dnia 29 kwietnia 2004r. 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. z 2004r. Nr 100 poz. 1024),
3. **Polityki Bezpieczeństwa Przetwarzania Danych Osobowych** w Urzędzie Miasta i Gminy w Kunowie.
4. **Instrukcji Zarządzania Systemem Informatycznym,** służącym do przetwarzania danych w Urzędzie Miasta i Gminy w Kunowie.
5. **Instrukcji Zarządzania Systemem Informatycznym,** służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Kunowie.

<u>Jednocześnie w czasie wykonywania swoich obowiązków służbowych zobowiązuję się do:</u>

a) zapewnienia ochrony danych osobowych przetwarzanych w Urzędzie Miasta i Gminy w Kunowie, a w szczególności zapewnienia ich bezpieczeństwa przed udostępnianiem osobom nieuprawnionym, zabraniem, uszkodzeniem oraz nieuprawnioną modyfikacją lub zniszczeniem,
b) zachowania w tajemnicy, także po ustaniu stosunku pracy, wszelkich informacji dotyczących ochrony fizycznej, technicznej i organizacyjnej danych osobowych, funkcjonowania systemów i urządzeń służących do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Kunowie,
c) zachowania w tajemnicy hasła dostępu do systemów informatycznych, przetwarzających dane osobowe w Urzędzie Miasta i Gminy w Kunowie, również po upływie jego ważności,
d) natychmiastowego zgłaszania przełożonemu i **Administratorowi Bezpieczeństwa Informacji** stwierdzenia na swoim stanowisku pracy próby lub faktu naruszenia zabezpieczenia fizycznego pomieszczenia, bezpieczeństwa danych osobowych lub systemu informatycznego, w którym przetwarzane są dane osobowe.

Kunów, dn. .....

.....
(podpis pracownika)

BURMISTRZ
mgr Leck Łodej

BURMISTRZ
Miasta i Gminy Kunów

Załącznik nr 2
do Instrukcji Zarządzania Systemem Informatycznym
w UMiG w Kunowie

Wniosek o nadanie uprawnień w systemie informatycznym

Rodzaj zmiany w systemie informatycznym:

☐ Nowy użytkownik ☐ Modyfikacja uprawnień ☐ Odebranie uprawnień

Imię i nazwisko użytkownika	
Opis zakresu uprawnień użytkownika w systemie informatycznym	

Data złożenia: .....

Data akceptacji:

.....
(czytelny podpis wnioskodawcy)

.....
(Akceptacja ABI)

BURMISTRZ
mgr Lech Łodej

BURMISTRZ
Miasta i Gminy Kunów

Załącznik nr 3
do Instrukcji Zarządzania Systemem Informatycznym
w UMiG w Kunowie

UPOWAŻNIENIE

NR .....

na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. z 2014 r. poz. 1182 z późn. zm.).

upoważniam

Panią/ Pana* .....

do przetwarzania danych osobowych

w ramach .....

(nazwa zbioru danych osobowych, nazwa zbioru tworzonego doraźnie do celów technicznych, nazwa rodzaju spraw związanych z przetwarzaniem danych osobowych poza zbiorem w systemach informatycznych w celu edycji/**)

Przetwarzanie danych osobowych może odbywać się przy wykorzystaniu:

.....

.....

(systemu informatycznego, systemu w postaci papierowej)

w zakresie .....

.....

(nazwa uprawnień w zakresie przetwarzania danych)

Upoważnienie jest ważne w czasie zatrudnienia użytkownika u Administratora Danych Osobowych lub do zmiany zakresu obowiązków użytkownika, lub do ustania realizacji zadań z których wynika brak potrzeby przetwarzania danych osobowych w zbiorze lub zakresie określonym upoważnieniem.

.....
(Administrator Danych Osobowych)

Kunów, dnia .....

/* niepotrzebne skreślić
/** właściwe podkreślić

BURMISTRZ
mgr Lech Łodej

BURMISTRZ
Miasta i Gminy Kunów

Załącznik nr 4
do Instrukcji Zarządzania Systemem Informatycznym
w UMiG w Kunowie

Rejestr użytkowników i ich uprawnień w systemie informatycznym

Lp.	Nazwisko i imię (Identyfikator)	System/aplikacja/zbiór danych osobowych	Data nadania upoważnienia	Data ustania upoważnienia
1				
2				
3				
4				
5				
6				
7				
8				

BURMISTRZ
mgr Tech Łodej

BURMISTRZ
Miasta i Gminy Kunów

Załącznik nr 5
do Instrukcji Zarządzania Systemem Informatycznym
w UMiG w Kunowie

Rejestr nośników komputerowych zawierających ważne dane

Lp.	Rodzaj nośnika i jego oznaczenie (sygnatura)	Krótki opis treści wykonanej kopii bezpieczeństwa	Data utworzenia kopii	Data zniszczenia kopii	Podpis ASI	Podpis ABI
1						
2						
3						
4						
5						
6						
7						
8						
9						

BURMISTRZ
mgr Lech Łodej

BURMISTRZ
Miasta i Gminy Kunów

Załącznik nr 7
do Instrukcji Zarządzania Systemem Informatycznym
w UMiG w Kunowie

Dziennik systemu informatycznego
Urzędu Miasta i Gminy w Kunowie

Dziennik zawiera opis wszelkich zdarzeń istotnych dla działania systemu informatycznego, a w szczególności:

- w przypadku awarii – opis awarii, przyczynę awarii, szkody wynikłe na skutek awarii, sposób usunięcia awarii, opis systemu po awarii, wnioski;
- w przypadku konserwacji systemu – opis podjętych działań, wnioski.

Lp.	Data i godzina zdarzenie	Opis zdarzenia	Podjęte działania	Podpis
1				
2				
3				
4				
5				
6				

BURMISTRZ
mgr Lech Łodej