Załącznik Nr 2 do Zarządzenia Burmistrza
Nr0050.58.2016 z dnia 23 czerwca 2016 r.

URZĄD MIEJSKI GMINY ŁOBŻENICA

INSTRUKCJA ZARZADZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE MIEJSKIM GMINY ŁOBŻENICA

ZATWIERDZAM
BURMISTRZ
Piotr Łosoś
.....

OPRACOWAŁ:

Administrator Bezpieczeństwa Informacji
w Urzędzie Miejskim Gminy w Łobżenicy

Łobżenica, dnia 23 czerwca 2016 roku.

§ 1.

POSTANOWIENIA OGÓLNE

Instrukcja zarządzania systemem informatycznym opracowana została zgodnie z wymogami § 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych w systemach informatycznych.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie zwana dalej „Instrukcją", określa:

1) zasady , tryb postępowania i zalecenia Administratora Danych Osobowych , które należy stosować w trakcie przetwarzania danych osobowych w systemach informatycznych,
2) sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz osoby odpowiedzialne za te czynności,
3) sposób rejestrowania i wyrejestrowywania użytkowników oraz osoby odpowiedzialne za te czynności,
4) zasady i procedury rozpoczynania i kończenia pracy,
5) zasady i częstotliwość tworzenia kopii bezpieczeństwa.
6) zasady i częstotliwość kontroli obecności wirusów komputerowych oraz metodę ich usuwania,
7) zasady i czas przechowywania nośników informacji, w tym kopii informatycznych,
8) zasady dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych,
9) zasady postępowania w zakresie komunikacji w sieci komputerowej.

§ 2.

DEFINICJE ZAWARTE W INSTRUKCJI

Ilekroć w instrukcji jest mowa o :

1) **ustawa** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r., poz. 2135 z późn. zm.), zwaną dalej *„ustawą"*;
2) **jednostka, Urząd** – rozumie się przez to Urząd Miejski Gminy w Łobżenicy;
3) **identyfikator użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
4) **hasło** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

5) **sieć telekomunikacyjna** – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (tj.Dz. U. z 2014 r., poz. 243, 827, 1198);
6) **sieć publiczna** – rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne;
7) **teletransmisja** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
8) **rozliczalność** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
9) **integralność danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
10) **raport** – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
11) **poufność danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
12) **uwierzytelnianie** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
13) **Administrator Danych Osobowych (ADO)** – w świetle przepisów ustawy o ochronie danych osobowych, art. 3 i 7 pkt 4 rozumie się przez to Burmistrza Łobżenicy, który decyduje o celach i środkach przetwarzania danych osobowych;
14) **Administrator Bezpieczeństwa Informacji (ABI)** – rozumie się przez to osobę wyznaczoną przez Administratora Danych, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
15) **Administrator Systemu Informatycznego (ASI), zwany też Administratorem Systemu** – rozumie się przez to osobę zatrudnioną przez Administratora Danych, upoważnioną do realizacji zadań związanych z zarządzaniem systemem informatycznym;
16) **użytkownik systemu informatycznego** – rozumie się przez to upoważnionego przez Administratora Danych, pracownika wyznaczonego do przetwarzania danych osobowych w systemie informatycznym, który odbył stosowne szkolenie w zakresie ochrony danych.

§ 3.

ZABEZPIECZENIE INFRASTRUKTURY INFORMATYCZNEJ I TELEKOMUNIKACYJNEJ

1. Zastosowano zasilacze awaryjne UPS do serwera, kluczowych komputerów na których są przetwarzane dane osobowe oraz do elementów sieci informatycznej takich jak: routery, modemy, przełączniki.

2. Dostęp do komputera przenośnego wynoszonego poza obszar Urzędu, zawierającego dane osobowe odbywa się poprzez podanie loginu i hasła

3. Użytkownicy komputerów przenośnych wynoszonych poza obszar Urzędu, na których są przetwarzane dane osobowe są zobowiązani do przestrzegania zasad bezpieczeństwa i podpisania załącznika Nr 1 do Instrukcji – „Regulamin użytkowania komputerów przenośnych".

4. Dane osobowe na komputerach przenośnych wynoszonych poza Urząd muszą być przechowywane na zaszyfrowanych partycjach.

5. W przypadku dostępu do danych osobowych przez Internet, stosuje się szyfrowanie tego połączenia (SSL lub VPN).

6. W przypadku dostępu do danych osobowych przez Internet do środków teletransmisji, wymagane jest uwierzytelnienie (podanie loginu i hasła).

7. Na serwerach zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.

8. Lokalizacja urządzeń komputerowych (komputerów typu PC, terminali, drukarek) uniemożliwia osobom niepowołanym dostęp do nich.

9. Dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej - komputerze przenośnym zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS.

10. Dostęp do stacji roboczych lub systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora i hasła.

11. Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.

12. Użyto system IDS/IPS do ochrony dostępu do sieci komputerowej.

§ 4.

ZABEZPIECZENIE PROGRAMÓW I APLIKACJI PRZETWARZAJĄCYCH DANE OSOBOWE

1. Dostęp do danych osobowych w programie lub w bazie wymaga uwierzytelnienia z wykorzystaniem identyfikatora i hasła.

2. Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.

3. Zastosowano mechanizm umożliwiający automatyczną rejestrację identyfikatora użytkownika i datę pierwszego wprowadzenia danych osobowych.

4. Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.

5. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.

6. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.

7. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika (automatyczny wygaszacz ekranu po 15 minutach).

§ 5.

ZASADY DOSTĘPU UŻYTKOWNIKA DO SYSTEMU

1. Dostęp o systemu informatycznego służącego do przetwarzania danych osobowych, zwanego dalej, „systemem" otrzymują osoby (użytkownicy), po uzyskaniu Upoważnienia do przetwarzania danych podpisanego przez Administratora Danych Osobowych, stanowiącego załącznik Nr 2 do Polityki bezpieczeństwa oraz podpisaniu Oświadczenia o poufności stanowiącego załącznik Nr 1 do Polityki bezpieczeństwa.

2. Użytkownik systemu informatycznego otrzymuje do niego dostęp po zarejestrowaniu w tym systemie przez Administratora Systemu na wniosek kierownika komórki organizacyjnej i po akceptacji Administratora Bezpieczeństwa Informacji.

3. Rejestracja, o której mowa w ust. l, polega na nadaniu identyfikatora przez ABI oraz przydzieleniu pierwszego hasła i wprowadzeniu tych danych do bazy użytkowników systemu przez ASI.

4. Wzór ewidencji zarejestrowanych użytkowników systemu, prowadzonej przez Administratora Systemu stanowi załącznik Nr 2 do Instrukcji.

§ 6.
IDENTYFIKATOR UŻYTKOWNIKA SYSTEMU

1. Identyfikator (login), który przydziela Administrator Bezpieczeństwa Informacji składa się z minimum pięciu znaków. W identyfikatorze pomija się polskie znaki diakrytyczne.

2. Każdy użytkownik musi posiadać swój własny indywidualny identyfikator.

3. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielony innej osobie.

§ 7.
HASŁA UŻYTKOWNIKA SYSTEMU

1. ASI informuje użytkownika systemu o nadaniu pierwszego hasła do systemu.

2. Użytkownik systemu zobowiązany jest do niezwłocznej zmiany tego hasła.

3. Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

4. Hasło nie może być identyczne z identyfikatorem użytkownika, ani z jego imieniem lub nazwiskiem.

5. Zmiana hasła następuje nie rzadziej niż co 30 dni.

6. Użytkownik systemu zobowiązuje się do zachowania hasła w poufności.

7. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.

§ 8.
WYREJESTROWANIE UŻYTKOWNIKA SYSTEMU

1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje Administrator Systemu na wniosek kierownika komórki organizacyjnej po uzgodnieniu z Administratorem Danych.

2. Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter czasowy lub trwały.

3. Wyrejestrowanie następuje poprzez:

1) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),

2) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

4. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego jest:

1) nieobecność w pracy trwająca dłużej niż 31 dni kalendarzowych,
2) zawieszenie w pełnieniu obowiązków służbowych,
3) zwolnienie z pełnienia obowiązków służbowych.

5. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy użytkownika.

§ 9.
HASŁA ADMINISTRATORA

1. Hasło administratora składa się z co najmniej ośmiu znaków. Powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

2. Hasło winien znać tylko administrator. Metryka hasła prowadzona przez administratora musi zawierać: treść hasła, datę jego wprowadzenia do systemu, datę i powód awaryjnego udostępnienia hasła oraz być przechowywane przez okres 5 lat.

3. Administrator zobowiązany jest do umieszczania haseł administratora w zamkniętych kopertach w sejfie Urzędu.

4. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.

5. Administrator Systemu Informatycznego może posiadać zastępcę. Zastępca ASI posługuje się własnym identyfikatorem i hasłem.

6. W przypadkach awaryjnych (np. nieobecności administratora) hasło administratora przechowywane w sejfie może być przekazane decyzją ADO osobie usuwającej skutki awarii. Po ustaniu sytuacji awaryjnej, administrator jest zobowiązany do zmiany hasła.

§ 10.
ROZPOCZĘCIE I ZAKOŃCZENIE PRACY W SYSTEMIE

1. Użytkownik rozpoczynający pracę zobowiązany jest przestrzegać procedur, które maja na celu sprawdzenie zabezpieczenia pomieszczenia, w którym przechowywane są dane osobowe, swojego stanowiska pracy oraz sprzętu komputerowego, a w szczególności:

1) przed wejściem do pomieszczenia sprawdzić czy na drzwiach i zamkach nie ma widocznych śladów prób niepowołanego ich otwierania,
2) sprawdzić stan okna i krat (jeżeli występują) oraz ocenić czy w pomieszczeniu nie ma znaków wskazujących na pobyt w nim osób nieuprawnionych,

3) sprawdzić stan sprzętu informatycznego oraz zamknięcie szaf i biurek.

2. Użytkownik przed przystąpieniem do przetwarzania danych w systemie winien:

1) zalogować się w systemie, posługując się swoim identyfikatorem i hasłem,
2) po zalogowaniu ocenić prace systemu i stan zbiorów danych.

3. Osoba użytkująca system informatyczny lub aplikacje, w których przetwarzane są dane osobowe powinien stosować przedsięwzięcia zapewniające bezpieczeństwo danych osobowych:

1) ustawić ekrany monitorów pomieszczeniu tak, aby uniemożliwić podgląd osób nieuprawnionych,
2) stosować automatyczne wygaszacze ekranu z ustawioną opcją wymagania hasła, które po upływie maksymalnie 15 minut nieaktywności użytkownika automatycznie wyłączają możliwość eksploracji ekranu.

4. Po zakończeniu pracy użytkownik powinien przestrzegać następujących zasad:

1) wylogować się z systemu i zaczekać na jego wyłączenie się,
2) sprawdzić czy nie zostały pozostawione bez nadzoru nośniki informacji,
3) upewnić się, że szafy i biurka z dokumentacja są zamknięte,
4) wyłączyć odbiorniki energii elektrycznej, zamknąć pomieszczenie.

§ 11.

ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZETU STACJONARNEGO

1. Sprzęt komputerowy służący do przetwarzania zbioru danych osobowych składa się z komputerów stacjonarnych, serwerów, drukarek.

2. Użytkownik zobowiązany jest korzystać ze sprzętu komputerowego w sposób zgodny z jego przeznaczeniem i chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem.

3. Użytkownik zobowiązany jest do zabezpieczenia sprzętu komputerowego przed dostępem osób nieupoważnionych a w szczególności zawartości ekranów monitorów.

4. Samowolne otwieranie (demontaż) sprzętu komputerowego, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) do lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.

§ 12.

ZASADY KORZYSTANIA Z OPROGRAMOWANIA

1. Użytkownik zobowiązuje się do korzystania wyłącznie z oprogramowania objętego prawami autorskimi.

2. Użytkownik nie ma prawa kopiować oprogramowania zainstalowanego na sprzęcie komputerowym na swoje własne potrzeby ani na potrzeby osób trzecich.

3. Instalowanie jakiegokolwiek oprogramowania na sprzęcie komputerowym może być dokonane wyłącznie przez Administratora Systemu lub osobę upoważnioną.

4. Użytkownicy nie mają prawa do instalowania ani używania oprogramowania innego, niż przekazane lub udostępnione im przez ASI. Zakaz dotyczy między innymi instalacji oprogramowania z zakupionych dyskietek, płyt CD, programów ściąganych ze stron internetowych, a także odpowiadania na samoczynnie pojawiające się reklamy internetowe.

5. Użytkownicy nie mają prawa do zmiany parametrów systemu, które mogą być zmienione tylko przez ASI lub osobę upoważniona.

6. W przypadku naruszenia któregokolwiek z powyższych postanowień Administrator Systemu ma prawo niezwłocznie i bez uprzedzenia usunąć nielegalne lub niewłaściwie zainstalowane oprogramowanie.

7. Za aktualizację oprogramowania zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje) odpowiada Administrator Systemu.

8. ASI odpowiada za zapewnienie licencjonowanego oprogramowania do przetwarzania danych osobowych.

§ 13.

ZASADY KORZYSTANIA Z INTERNETU

1. Użytkownik winien korzystać z Internetu wyłącznie w celach służbowych.

2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą Administratora Systemu i tylko w uzasadnionych przypadkach.

3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.

4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo.

5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.

6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:".

7. Należy zachować szczególną ostrożność w przypadku żądania lub prośby podania kodów, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.

8. Użytkownicy mogą także korzystać z Internetu dla celów prywatnych, ale wyłącznie okazjonalnie i powinno być ono ograniczone do niezbędnego minimum.

9. Korzystanie z Internetu dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.

10. Przy korzystaniu z Internetu, użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.

11. W zakresie dozwolonym przepisami prawa, ADO zastrzega sobie prawo kontrolowania sposobu korzystania przez użytkownika z internetu pod kątem wyżej opisanych zasad.

12. Ponadto, w uzasadnionym zakresie, ADO zastrzega sobie prawo kontroli czasu spędzanego przez użytkownika w Internecie.

§ 14.

ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Służbowa poczta elektroniczna jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.

2. W przypadku przesyłania danych wrażliwych, wewnątrz Urzędu bądź wszelkich danych osobowych poza Urząd należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych plików, podpis elektroniczny).

3. Przy zabezpieczeniu plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.

4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.

5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych e-mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.

6. Nie należy otwierać załączników (plików) w e-mailach nadesłanych przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę.

7. Nie należy otwierać stron internetowych wskazanych hiperłączami w e-mailach, gdyż mogą to być odnośniki do stron zainfekowanych lub niebezpiecznych.

8. Użytkownicy nie powinni rozsyłać za pośrednictwem e-maila informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia", itp.

9. Użytkownicy nie powinni rozsyłać, e-maili zawierających załączniki o dużym rozmiarze.

10. Użytkownicy powinni okresowo kasować niepotrzebne e-maile.

11. Podczas wysyłania e-maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW".

12. Przy korzystaniu z e-maila, użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego

13. Użytkownicy nie mają prawa korzystać z e-maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania

§ 15.

ZABEZPIECZENIE DOKUMENTÓW I WYDRUKÓW

1. Dokumenty i wydruki trwałe z danymi osobowymi przechowuje się w archiwum lub w zabezpieczonych fizycznie pomieszczeniach, biurkach i szafach.

2. Pracownicy są zobowiązani do zabezpieczania dokumentów (np. zamykanie dokumentów na klucz w szafach, biurkach) przed dostępem osób nieupoważnionych podczas swojej nieobecności w pomieszczeniach lub po zakończeniu pracy (tzw. Polityka czystego biurka).

3. Zabrania się pozostawiania wydruków oraz ksero na drukarkach, skanerach i kserokopiarkach bez nadzoru.

4. Niszczenie dokumentów zawierających dane osobowe, w tym wydruków tymczasowych musi odbywać się z użyciem niszczarek.

5. Za zapewnienie bezpieczeństwa dokumentów i wydruków odpowiedzialni są kierownicy właściwych komórek organizacyjnych oraz podległe im osoby przetwarzające dane osobowe.

§ 16.

PROCEDURA TWORZENIA KOPII ZAPASOWYCH

Administrator Systemu Informatycznego przestrzega niżej wymienionej procedury dotyczącej częstotliwości tworzenia kopii zapasowych:

1) Zbiory danych osobowych oraz programy i narzędzia programowe służące do ich przetwarzania, zapisywanie na nośnikach zewnętrznych (np. dyski: wymienne, magnetyczne, optyczne) tworzące kopie zapasowe kolejnych okresów, powinny być odpowiednio oznakowane i przechowywane w wyznaczonych, odpowiednio zabezpieczonych pomieszczeniach.
2) Kopie zapasowe określone w pkt.1 powinny być sporządzane regularnie w okresach wyznaczonych niżej w pkt. 3.
3) Ustala się następującą częstotliwość tworzenia kopii awaryjnych na nośnikach zewnętrznych – magnetycznych i optycznych:
   a) Kopie tygodniowe, wykonywane przez ASI lub użytkowników obejmujące:
      - dane finansowe
   b) Kopie miesięczne, umieszczane w zapieczętowanych kopertach, deponowane przez ASI w miejscu wyznaczonym i odpowiednio zabezpieczonym obejmują:
      - dane finansowe,
      - stacje robocze.
   c) Kopie tygodniowe przechowywane są do czasu zdeponowania kopii miesięcznych,
   d) Kopie miesięczne przechowywane są do czasu zdeponowania kopii rocznej.
   e) Niszczenie kopii awaryjnych należy wykonać w sposób określony w instrukcji zachowując szczególna ostrożność przed wydostaniem się informacji na zewnątrz lub w niepowołane ręce.
   f) W sytuacjach awaryjnych zaistniałych pod nieobecność ASI lub w razie jego niedyspozycji Administrator Danych udostępnia kopie awaryjne osobie przez siebie wyznaczonej i upoważnionej.

§ 17.

ZABEZPIECZENIE ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI

1. Nośniki informacji zawierające dane osobowe, w tym zawierające kopie zapasowe, Administrator Systemu rejestruje w „Rejestrze nośników informacji zawierających ważne dane". Wzór rejestru przedstawia załącznik Nr 3 do niniejszej Instrukcji

2. Nośniki danych są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych.

3. Zabrania się wynoszenia poza obszar Urzędu wymiennych nośników informacji a w szczególności twardych dysków z zapisanymi danymi osobowymi i pendrive bez zgody ADO.

4. Dane osobowe wynoszone poza obszar Urzędu na nośnikach elektronicznych muszą być zaszyfrowane.

5. W sytuacji przekazywania nośników z danymi osobowymi poza Urząd można stosować następujące zasady bezpieczeństwa:

   a. adresat powinien zostać powiadomiony o przesyłce,
   b. dane przed wysłaniem powinny zostać zaszyfrowane a hasło podane adresatowi inną drogą,
   c. stosować bezpieczne koperty depozytowe,
   d. przesyłkę należy przesyłać przez kuriera.

6. Osoby wykorzystujące nośniki zobowiązane są do niezwłocznego i trwałego usuwania (kasowania) danych osobowych po ustaniu celu ich przechowywania (chyba, że z powodu odrębnych przepisów należy dane zachowywać).

7. Podlegające likwidacji uszkodzone lub przestarzałe nośniki a szczególności twarde dyski z danymi osobowymi są komisyjnie niszczone w sposób fizyczny. Wzór protokołu zniszczenia uszkodzonych nośników informacji stanowi załącznik Nr 4 do Instrukcji.

8. Nośniki informacji zamontowane w sprzęcie komputerowym a w szczególności twarde dyski z danymi osobowymi powinny być wymontowane lub wyczyszczone specjalistycznym oprogramowaniem, zanim zostaną przekazane poza Urząd (np. sprzedaż lub darowizna komputerów stacjonarnych / laptopów).

9. Osoby wykorzystujące elektroniczne nośniki z danymi osobowymi są zobowiązane do zabezpieczeniach ich (w szafach, biurkach) przed dostępem osób nieupoważnionych, szczególnie poza godzinami pracy (tzw. Polityka czystego biurka).

§ 18.

OCHRONA ANTYWIRUSOWA

Celem procedury jest zabezpieczenie systemów informatycznych przed szkodliwym oprogramowaniem (np. typu robaki, wirusy, konie trojańskie, rootkity) oraz nieautoryzowanym dostępem do systemów przetwarzających dane osobowe.

1. Za zaplanowanie i zapewnienie ochrony antywirusowej odpowiada ASI, w tym za zapewnienie odpowiedniej ilości licencji dla użytkowników.
2. System antywirusowy zainstalowano na serwerze oraz na stacjach roboczych.
3. System antywirusowy zapewnia ochronę: systemu operacyjnego, przechowywanych plików, poczty wychodzącej i przychodzącej.
4. Użytkownicy zobowiązani są do skanowania plików programem antywirusowym.
5. ASI zapewnia stałą aktywność programu antywirusowego, tzn. program antywirusowy musi być aktywny podczas pracy systemu informatycznego przetwarzającego dane osobowe.
6. Aktualizacja definicji wirusów odbywa się automatycznie przez zainstalowany program antywirusowy.
7. W przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik winien powiadomić ASI.

§ 19.

OCHRONA PRZED NIEAUTORYZOWANYM DOSTĘPEM DO SIECI LOKALNEJ

Stosowane zabezpieczenia mają na celu zabezpieczenie systemów informatycznych przed nieautoryzowanym dostępem do sieci lokalnej np. przez programy szpiegujące, hackerów.

1. Za zaplanowanie, konfigurowanie, aktywowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku sieci lokalnej i sieci rozległej odpowiada Administrator Systemu.
2. Stosowany jest Firewall sprzętowy i programowy na serwerze i na stacjach roboczych.
3. Zastosowano mechanizmy kontroli dostępu do sieci w postaci: IDS/IPS do wykrywania i blokowania ataków do sieci komputerowej, technikę NAT.
4. Sieć bezprzewodową zabezpieczono technologią WPA.

5. Zastosowano mechanizmy monitorujące przeglądanie Internetu przez użytkowników. Uwzględniają one:

- Blokowanie stron internetowych określonego typu.
- Blokowanie określonych stron internetowych,
- Analizę przesyłanych informacji pod kątem niebezpiecznego oprogramowania.

§ 20.
PRZEGLĄDY I KONSERWACJE SYSTEMU INFORMATYCZNEGO I APLIKACJI

Celem procedury jest zapewnienie ciągłości działania systemów informatycznych przetwarzających dane osobowe oraz zabezpieczenie danych osobowych przed ich nieuprawnionym udostępnieniem.

1. ASI odpowiada za bezawaryjną pracę systemu komputerowego, w tym: stacji roboczych, aplikacji serwerowych, baz danych, poczty email.

2. Przegląd i konserwacja systemu informatycznego powinny być wykonywane w terminach określonych przez producentów systemu lub zgodnie z harmonogramem ASI, jednak nie rzadziej, niż raz w roku.

3. Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI.

4. ASI odpowiada za optymalizację zasobów serwerowych, wielkości pamięci i dysków.

5. ASI odpowiada za sprawdzanie poprawności działania systemu komputerowego, w tym: stacji roboczych, serwerów, drukarek, baz danych, poczty email.

6. ASI odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia.

7. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego, wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.

8. Czynności konserwacyjne i naprawcze wykonywane doraźnie przez osoby nie posiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych), muszą być wykonywane pod nadzorem osób upoważnionych.

9. Przed przekazaniem uszkodzonego sprzętu komputerowego z danymi osobowymi do naprawy poza teren organizacji, należy:

a. wymontować nośniki z danymi osobowymi,
b. trwale usunąć dane osobowe z użyciem specjalistycznego oprogramowania,
c. nadzorować proces naprawy przez osobę upoważnioną przez administratora systemu, gdy nie ma możliwości usunięcia danych z nośnika.

§ 21.
ODPOWIEDZIALNOŚĆ

Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.

§ 22.
PRZEPISY KOŃCOWE

W sprawach nieuregulowanych w niniejszej Instrukcji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 r. poz. 1182, 1662) 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. z 2015 r., poz. 2135 z późn. zm.).

Załącznik Nr 1 do Instrukcji – Regulamin użytkowania komputerów przenośnych

REGULAMIN UŻYTKOWANIA KOMPUTERÓW PRZENOŚNYCH

1) Każdy Użytkownik komputera przenośnego winien zapoznać się z Regulaminem użytkowania komputerów przenośnych oraz pisemnie zobowiązać się do jego przestrzegania.
2) W przypadku przechowywania na komputerze przenośnym danych osobowych lub stanowiących tajemnicę Urzędu, Użytkownik zobowiązany jest do ich przechowywania na dysku szyfrowanym, zabezpieczonym co najmniej 8 znakowym hasłem (duże, małe litery, znaki specjalne lub cyfry).
3) Na komputerach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny, o ile jest to możliwe, znajdować się dane osobowe lub stanowiące tajemnicę Urzędu.
4) W przypadku kradzieży lub zgubienia komputera przenośnego, Użytkownik powinien natychmiast powiadomić o tym Administratora Bezpieczeństwa Informacji, zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.
5) Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego w czasie transportu, a w szczególności:
   a) zaleca się przenoszenie go w specjalnej teczce,
   b) zabrania się pozostawiania komputera przenośnego w samochodzie podczas postoju w miejscu publicznym bez nadzoru.
6) W przypadku, gdy komputer przenośny pozostawiony jest w miejscu dostępnym dla osób nieupoważnionych, Użytkownik jest zobowiązany do stosowania kabla zabezpieczającego. W szczególności dotyczy to zabezpieczenia komputera na stanowisku pracy, podczas konferencji, prezentacji, szkoleń, targów itp.
7) W przypadku pozostawiania komputerów przenośnych w biurze zaleca się umieszczanie ich po zakończeniu pracy w zamykanych szafkach.
8) Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze lub na określonych nośnikach (pendrive, CD, DVD). Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem osób niepowołanych.
9) Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, Użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.

Zapoznałem się z treścią Regulaminu użytkowania komputerów przenośnych i zobowiązuję się do przestrzegania zasad w nim zawartych.

.....
(data i czytelny podpis Użytkownika)

Załącznik Nr 2 do Instrukcji – Ewidencja zarejestrowanych użytkowników systemu informatycznego

EWIDENCJA ZAREJESTROWANYCH UŻYTKOWNIKÓW SYSTEMU INFORMATYCZNEGO

Lp.	Imię i nazwisko użytkownika systemu	Nazwa komórki organizacyjnej	Identyfikator	Data zarejestrowania w systemie	Data wyrejestrowania z systemu

Załącznik Nr 3 do Instrukcji – Rejestr nośników informacji zawierających ważne dane

REJESTR NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH WAŻNE DANE

Oznaczenie nośnika	Data wpisania w rejestr	Opis nośnika	Miejsce przechowywania nośnika	Podpis użytkownika	Uwagi

Oznaczenie nośnika:
Kolejny nr nośnika / symbol nośnika / symbol komórki organizacyjnej

Przykładowe symbole nośników:
T – taśma; **D** – dyskietka; **Z** – zip; **CD** – płyta CD lub DVD; **P** – pendrive.

Załącznik Nr 4 do Instrukcji – Protokół zniszczenia uszkodzonych nośników informacji

.... dnia .....r.
(akcept powołującego komisję)

Protokół nr .....
zniszczenia uszkodzonych nośników informacji
w Urzędzie Miejskim Gminy w Łobżenicy

Dnia ..... komisja powołana przez Burmistrza Łobżenicy

w składzie:

1. Przewodniczący: .....
2. Członkowie: .....
   .....

dokonała trwałego zniszczenia nośników informacji:

L.p.	Nazwa	Nr ewidencyjny	Sposób zniszczenia	Uwagi

Dokonanie w/w czynności zostaje potwierdzone własnoręcznymi podpisami komisji:

.....

.....

.....

ADMINISTRATOR SYSTEMU

.....