Załącznik nr 2
Do Zarządzenia nr 17/2011

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

§1.
Cel instrukcji

Instrukcja określa sposób zarządzania systemem informatycznym wykorzystywanym do przetwarzania danych osobowych przez administratora danych w celu zabezpieczenia danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnianiem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem, opisuje nadawanie uprawnień użytkownikom, określa sposoby pracy w systemie informatycznym oraz czynności mające wpływ na zapewnienie bezpieczeństwa systemu informatycznego ŁZUK.

§2.

Poziom bezpieczeństwa

1. Uwzględniając kategorie danych osobowych oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie informatycznym połączonym z siecią publiczną, wprowadza się „poziom wysoki" bezpieczeństwa zgodnie z §6 rozporządzenia.

§3.
Nadawanie i rejestrowanie (wyrejestrowywanie) uprawnień do przetwarzania danych w systemie informatycznym

2. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z :
    a. Ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 ze zm.),
    b. Polityką bezpieczeństwa systemów informatycznych do przetwarzania danych osobowych w Łódzkim Zakładzie Usług Komunalnych
    c. niniejszym dokumentem,
    d. oraz posiadać upoważnienie do przetwarzania danych osobowych.

3. Administrator Systemu Informatycznego przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego upoważnienia (wniosku) określającego zakres uprawnień pracownika, którego wzór stanowi **załącznik nr 1**,

4. Administrator Systemu jest zobowiązany upoważnić co najmniej jednego pracownika - do rejestracji użytkowników w systemie informatycznym w czasie swojej nieobecności.

5. Rejestracja użytkownika, polega na nadaniu unikalnego identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.

6. Wyrejestrowanie użytkownika z systemu informatycznego dokonuje administrator systemu na wniosek przełożonego **załącznik nr 1**, któremu pracownik podlega z podaniem daty oraz przyczyny odebrania uprawnień, zatwierdzonego przez Administratora bezpieczeństwa informacji.

7. Wyrejestrowanie, o którym mowa w pkt.6, może mieć charakter czasowy lub trwały.

8. Wyrejestrowanie następuje przez:
   9. zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe)
   10. usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

11. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego może być:
    a. wypowiedzenie umowy o pracę;
    b. wszczęcie postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych osobowych.
    c. zawieszenie w pełnieniu obowiązków służbowych

12. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.

13. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jej hasło.

14. Administrator Systemu Informatycznego zobowiązany jest do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym, rejestr stanowi **załącznik nr 2**.

§4.
Metody i środki uwierzytelniania oraz procedury związane z ich zarządzeniem i użytkowaniem

1. Identyfikator składa się z co najmniej dwu znaków, z których pierwszy znak odpowiada pierwszej literze imienia użytkownika pisanej dużymi literami, a drugi znak odpowiada pierwszej literze nazwiska pisanej dużymi literami. W identyfikatorze pomija się polskie znaki diakrytyczne.

2. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika administrator systemu. Za zgodą administratora bezpieczeństwa informacji, nadaje inny identyfikator odstępując od zasady określonej w §13.

3. W systemie stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji.

4. Identyfikator użytkownika w aplikacji (o ile działanie aplikacji na to pozwala), powinien być tożsamy z tym, jaki jest mu przydzielany w sieci lokalnej.

5. Kierownicy komórek organizacyjnych zobowiązani są pisemnie informować Administratora Bezpieczeństwa Informacji o każdej zmianie dotyczącej podległych pracowników mających wpływ na zakres posiadanych uprawnień w systemie informatycznym.

6. Bezpośredni dostęp do systemu informatycznego może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.

7. Hasło użytkownika powinno być zmieniane nie rzadziej niż co 30 dni.

8. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.

9. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.

10. Hasło użytkownika utrzymuję się również w tajemnicy po upływie ich ważności.

11. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.

12. W sytuacji kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do powiadomienia Administratora Systemu w celu nadania nowego hasła.

13. Hasło powinno składać się z niepowtarzalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne o ile system informatyczny na to pozwala. Hasło nie może być identyczne z identyfikatorem użytkownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, itp.), ani z jego imieniem lub nazwiskiem.

14. Zakazuje się stosować haseł, które użytkownik stosował uprzednio w okresie minionego roku, imion osób z najbliższej rodziny, ogólnie dostępnych informacji o użytkowniku takich jak numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy na której mieszka lub pracuje, przewidywanych sekwencji z klawiatury (np.: „QWERTY” i „12345” itp.

15. Zmiany hasła nie wolno zlecać innym osobom, oprócz Administratora Systemu..

16. Nie należy korzystać opcji zapamiętywania hasła w systemie.

17. Hasło administratora systemu przechowywane jest w zamkniętej kopercie w sejfie ognioodpornym do którego mają dostęp wyłącznie Dyrektor ŁZUK, jego zastępcy, Administrator Systemu oraz Administrator Bezpieczeństwa Informacji.

§5.
Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

1. Rozpoczęcie pracy na stacji roboczej następuje po włączeniu napięcia w listwie podtrzymującej napięcie (w przypadku posiadania listwy), włączeniu zasilacza awaryjnego (UPS) i komputera, a następnie wprowadzeniu identyfikatora indywidualnego oraz hasła identyfikatora znanego tylko użytkownikowi,

2. W pomieszczeniu, w którym przetwarzane są dane osobowe, mogą znajdować się osoby postronne tylko za zgodą i w towarzystwie użytkownika albo Administratora Bezpieczeństwa Informacji,

3. Przed osobami postronnymi należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwiać podgląd), wydruki leżące na biurkach oraz w otwartych szafach,

4. Monitory komputerów wyposażone są we włączające po 10 minutach od przerwania pracy wygaszacze ekranu. Wznowienie wyświetlenia następuje dopiero po wprowadzeniu odpowiedniego hasła,

5. W przypadku opuszczenia stanowiska pracy użytkownik obowiązany jest wylogować się z systemu, aktywować wygaszać ekranu lub w inny sposób zablokować stację robocza,

6. Obowiązuje zakaz robienia kopii całych zbiorów danych. Całe zbiory danych mogą być kopiowane tylko przez Administratora Systemu lub automatycznie przez system, z zachowaniem procedur ochrony danych osobowych,

7. Jednostkowe dane mogą być przekazywane pocztą elektroniczną między komputerami Administratora Danych a komputerami przenośnymi użytkowników tylko po ich zabezpieczeniu hasłem.,

8. Wypisy ze zbiorów danych udostępniane na podstawie art. 29 ustawy podmiotom nie będącym odbiorcami danych można przesyłać poczta elektroniczną tylko w postaci zaszyfrowanej,

9. Obowiązuje zakaz wynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz obszernych z nich wypisów, nawet w postaci zaszyfrowanej,

10. Przetwarzając dane osobowe, należy odpowiednio często robić kopie robocze danych, na których się właśnie pracuje, tak aby zapobiegać ich utracie,

11. Zakończenie pracy na stacji roboczej następuje po wprowadzeniu danych programów, a następnie prawidłowym zamknięciu aplikacji uruchomionych oraz wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w zasilaczu awaryjnym (UPS) i listwie (jeżeli jest podłączona),

12. Przed opuszczeniem pokoju należy:

a. zniszczyć w niszczarce lub schować do zamykanych na klucz szaf wszelkie wykonane wydruki zawierające dane osobowe,
b. schować do zamykanych na klucz szaf akta zawierające dane osobowe,
c. zamknąć okna.

13. Opuszczając pokój, należy zamknąć za sobą drzwi na klucz. Jeśli niemożliwe jest umieszczenie wszystkich zawierających dane osobowe dokumentów w zamykanych szafach, to należy powiadomić o tym Administratora Danych Osobowych lub Kierownika Działu Administracyjnego, który zgłasza osobom sprzątającym jednorazową rezygnację z wykonania usługi sprzątania.

14. Jeżeli jest to możliwe, to przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują procedury określone w niniejszej instrukcji dotyczące pracy na komputerach stacjonarnych,

15. Użytkownicy, którym zostały powierzone komputery przenośne powinny chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych; szczególną ostrożność należy zachować podczas ich transportu,

16. Obowiązuje zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone,

17. Praca na komputerze przenośnym możliwa jest po wprowadzeniu hasła i indywidualnego identyfikatora użytkownika,

18. Użytkownicy są zobowiązani zmieniać hasła w komputerach przenośnych nie rzadziej niż co 30 dni,

19. Obowiązuje zakaz przetwarzania na komputerach przenośnych całych zbiorów danych lub obszernych z nich wypisów, nawet w postaci zaszyfrowanej,

20. Obowiązuje zakaz samodzielnej modernizacji oprogramowania i sprzętu w powierzonych komputerach stacjonarnych oraz przenośnych. Wszelkie zmiany mogą być dokonywane tylko pod nadzorem Administratora Systemu, stosownie do wymagań niniejszej instrukcji. W razie wystąpienia usterek w pracy komputerów przenośnych lub w razie wystąpienia konieczności aktualizacji ich oprogramowania należy zgłosić to Administratorowi Systemu,

21. Komputery stacjonarne oraz przenośne wyposażone są w odpowiednie programy ochrony antywirusowej, których aktualizację pobierana jest automatyczne lub przez Administratora Systemu.

§6.
Procedury tworzenia kopii zapasowych

1. Kopie zapasowe tworzy się:
   a. codziennie – w przypadku programu Xpertis, Ewgrob
   b. nie rzadziej niż raz na miesiąc – w wypadku zbioru programu Płatnik

2. raz w roku kalendarzowym robiona jest kopia na płytach DVD, jeżeli na to pozwala wielkość danych zgromadzonych w ciągu roku.

3. Wybrane kopie wykonywane są po zakończeniu pracy wszystkich użytkowników w sieci komputerowej.

4. Kopia bezpieczeństwa wykonywana jest na płytach CD/DVD lub innym nośniku danych.

5. W przypadku wykonywania zabezpieczeń długoterminowych na taśmach magnetycznych lub płytach CD/DVD, nośniki te należy dwa razy w roku sprawdzać pod kątem ich dalszej przydatności.

6. Stwierdzenie utraty przez nośniki danych waloru przydatności do wykonywania kopii bezpieczeństwa, upoważnia Administratora Systemu do ich zniszczenia.

§7.
Przechowywanie elektronicznych nośników informacji zawierających dane osobowe oraz wydruków ich kopii zapasowych

1. Elektroniczne nośniki informacji.
    a. Dane osobowe w postaci elektronicznej – zapisywane na dyskietkach, dyskach magnetooptycznych czy dyskach twardych nie są wynoszone poza siedzibę ŁZUK
    b. Wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych określonych w Polityce bezpieczeństwa systemów informatycznych do przetwarzania danych osobowych.
    c. Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych.
    d. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe uszkadza się w sposób mechaniczny uniemożliwiając ich odczytanie.
    e. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych pozbawia się wcześniej zapisu tych danych.
    f. 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 osoby upoważnionej.

2. Zakazuje się przetwarzania danych osobowych na zewnętrznych nośnikach magnetycznych, optycznych i innych oraz ich przesyłania pocztą, elektroniczną bez ich uprzedniego zaszyfrowania.

3. Na nośnikach, o których mowa w p.2 , dopuszczalne jest przetwarzanie jedynie jednostkowych danych osobowych.

4. W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym na swoim komputerze.

5. Nośniki magnetyczne z zaszyfrowanymi, jednostkowymi danymi osobowymi są – na czas ich użyteczności – przechowywane w zamkniętych na klucz szafach, a po ich wykorzystaniu dane na nich zawarte są trwale usuwane lub nośniki te są niszczone.

6. Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione do przetwarzania danych osobowych.

7. Kopie zapasowe programów, których przydatność nie nadaje się do dalszego wykorzystania są trwale niszczone mechanicznie w niszczarce.

8. Kopie zapasowe.

    a. Kopie zapasowe są przechowywane w szafie pancernej w pok. 201
    b. Dostęp do danych opisanych w punkcie 8.a ma Administrator Systemu Informatycznego.

9. Wydruki.
    a. W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.
    b. Pomieszczenia, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy.
    c. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

§8.
Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz wirusami komputerowymi

1. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe pracujące w trybie monitora (ciągła praca w tle).

2. Każdy e-mail oraz załączniki muszą być sprawdzone przez program antywirusowy pod kątem obecności wirusów.

3. Definicje wzorców wirusów aktualizowane są nie rzadziej niż raz w tygodniu

4. Do obowiązków Administratora Systemu należy aktualizacja oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji wirusów dokonywanych przez to oprogramowanie.

5. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć.

6. Zabrania się pobierania z internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.

7. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.

8. Administrator Systemu Informatycznego przeprowadza cyklicznie kontrole antywirusowe na wszystkich komputerach – minimum co trzy miesiące.

9. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku stwierdzenia nieprawidłowości zgłoszonych przez pracownika w funkcjonowaniu sprzętu komputerowego lub oprogramowania.

10. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe na którym wykryto wirusa oraz wszystkie posiadane przez użytkownika nośniki.

11. Użytkownik jest obowiązany zawiadomić administratora systemu o pojawiających komunikatach wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.

12. Użytkownicy mogą korzystać z zewnętrznych nośników danych tylko po uprzednim sprawdzeniu zawartości nośnika oprogramowaniem antywirusowym.

§9 .
Kontrola nad wprowadzaniem, dalszym przetwarzaniem i udostępnianiem danych osobowych

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom uprawnionym.

2. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną.

3.

4. Aplikacje danych osobowych do obsługi baz danych osobowych powinny zapewniać odnotowanie informacji o udzielonych odbiorcom danych. Zakres informacji powinien obejmować co najmniej dane odbiorcy, datę wydania, zakres udostępnionych danych.

§10.
Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

1. Przeglądu i konserwacji systemu dokonuje administrator systemu doraźnie.

2. Przeglądu i konserwacji urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonych przez producenta sprzętu.

3. Nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny powinny być przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić Administratora Bezpieczeństwa Informacji.

4. Przeglądu pliku zawierającego raport dotyczący działalność aplikacji bądź systemów serwerowych (log systemowy) Administrator Systemu dokonuje nie rzadziej niż raz na miesiąc.

5. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy współudziale Administratora Systemu nie rzadziej niż raz na miesiąc.

6. W przypadku działań konserwacyjnych, awarii oraz napraw Administrator Bezpieczeństwa Informacji prowadzi „Dziennik systemu informatycznego ŁZUK **załącznik nr 3**

7. Wpisów do dziennika może dokonywać Administrator Danych, Administrator Bezpieczeństwa Informacji lub Administrator Systemu Informatycznego

§11.
Naprawa urządzeń komputerowych z chronionymi danymi osobowymi

1. Wszelkie naprawy urządzeń komputerowych oraz zmiany w systemie informatycznym Administratora Danych przeprowadzane są – jeżeli jest to możliwe – przez Administratora Systemu .

2. Naprawy i zmiany w systemie informatycznym Administratora Danych przeprowadzane przez serwisanta prowadzone są pod nadzorem Administratora Systemu, jeżeli jest to możliwe – w siedzibie administratora danych lub poza siedzibą Administratora Danych, po uprzednim nieodwracalnym usunięciu danych w nich przetwarzanych, a jeśli wiązałoby się to z nadmiernymi utrudnieniami, to po podpisaniu umów powierzenia przetwarzania danych osobowych.

3. Jeśli nośnik danych (dysk, dyskietka, płyta lub inne) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, to należy go zniszczyć mechanicznie.

§12.
Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego

1. Użytkownik zobowiązany jest zawiadomić Administratora Systemu lub Administratora Bezpieczeństwa Informacji o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu, a w szczególności o :

    a. naruszeniu hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzania hasła),
    b. częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień,
    c. braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera,

d. wykryciu wirusa komputerowego,
e. zauważeniu elektronicznych śladów próby włamania do systemu informatycznego Administratora Danych,
f. znacznym spowolnieniu działu informatycznego,
g. podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe,
h. zmianie położenia sprzętu komputerowego,
i. zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf.

2. Do czasu przybycia na miejsce Administratora Bezpieczeństwa Informacji lub Administratora Systemu:

   a. jeżeli istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego zdarzenia a następnie uwzględnić w działaniu również ustalenie jego przyczyny lub sprawców,
   b. rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   c. zaniechać – jeżeli to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
   d. zastosować się do instrukcji i regulaminów lub dokumentacji aplikacji, jeśli odnoszą się one do zaistniałego przypadku,
   e. przygotować opis incydentu,
   f. nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji lub Administratora Systemu.

3. Administrator Systemu przyjmujący zawiadomienie jest obowiązany niezwłocznie poinformować Administratora Bezpieczeństwa Informacji o naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu.

4. Administrator Bezpieczeństwa Informacji po otrzymaniu zawiadomienia, o którym mowa w p.2, powinien niezwłocznie:
   a. przeprowadzić postępowanie wyjaśniające, w celu ustalenia okoliczności naruszenia ochrony danych osobowych,
   b. podjąć działania chroniące system przed ponownym naruszeniem,
   c. w przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu sporządzić raport naruszenia bezpieczeństwa systemu informatycznego Administratora Danych, a następnie niezwłocznie przekazać jego kopie Administratorowi Danych,

5. Administrator Bezpieczeństwa Informacji w uzgodnieniu z Administratorem Systemu Informatycznego może zarządzić, w razie potrzeby, odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części.

6. W razie odtwarzania danych z kopii zapasowych Administrator Systemu Informatycznego obowiązany jest upewnić się, że odtwarzane dane zapisane zostały przed wystąpieniem incydentu; dotyczy to zwłaszcza przypadków infekcji wirusowej.

7. Administrator danych po zapoznaniu się z raportem, o którym mowa w p.4.c, podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych, szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego Administratora Danych bądź zastosowaniu środków ochrony fizycznej.

8. Administrator Bezpieczeństwa Informacji i Administrator Systemu Informatycznego zobowiązani są do informowania Administratora Danych o awariach systemu informatycznego, zauważonych przypadkach naruszenia niniejszej instrukcji przez użytkowników, a zwłaszcza o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami, nieprzestrzegania zasad używania oprogramowania antywirusowego, niewłaściwego wykorzystania sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z procedurami ochrony danych osobowych.

9. Administrator Bezpieczeństwa Informacji składa raz w roku Administratorowi Danych kompleksową analizę zarządzania systemem informatycznym.

§13.
Postanowienia końcowe

1. W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.

2. Administrator Systemu Informatycznego może upoważnić inne osoby do realizacji w jego imieniu zadań związanych z bezpieczeństwem systemu informatycznego Zakładu. Upoważnienie może obejmować zadania związane z realizacją postanowień dotyczących rejestracji i usuwania użytkowników w systemie informatycznym Zakładu, przydzielania uprawnień użytkownikom oraz zarządzania komunikacją w sieci komputerowej, wykonywaniu kopii zapasowych, przyjmowania informacji o naruszeniu lub podejrzeniu naruszenia zasad przedstawionych w niniejszej instrukcji oraz innych czynności o charakterze technicznym niezbędnych do prawidłowego funkcjonowania systemu informatycznego.

3. Naruszenie obowiązków wynikających z niniejszej instrukcji oraz przepisów o ochronie danych osobowych może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym, w szczególności wynikającym z art. 49-54 ustawy.

Załącznik nr 1
do Instrukcji Zarządzania
Systemem Informatycznym

WNIOSEK
O NADANIE UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

☐ Nowy użytkownik	☐ Modyfikacja uprawnień	☐ Odebranie uprawnień w systemie Informatycznym

Imię i nazwisko użytkownika:	**Wydział/biuro/samodzielne stanowisko**
Opis i zakres uprawnień użytkownika w systemie informatycznym	
Data wystawienia:	Podpis bezpośredniego przełożonego użytkownika systemu:
Podpis Administratora Systemu:	Akceptacja ABI

Załącznik nr 2
do Instrukcji Zarządzania Systemem Informatycznym

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRACY W SYSTEMIE INFORMATYCZNYM ORAZ UPOWAŻNINYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Nazwisko, Imię	System/aplikacja	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania uprawnień	Data ustania uprawnień	Identyfikator użytkownika

Załącznik nr 3
do Instrukcji Zarządzania
Systemem Informatycznym

Dziennik zawiera opisy wszelkich zdarzeń istotnych dla działania systemu informatycznego w szczególności:
- w przypadku awarii – opis awarii, przyczyna awarii, szkody wynikłe na skutek awarii, sposób usunięcia awarii, opis systemu po awarii, wnioski,
- w przypadku konserwacji systemu – opis podjętych działań, wnioski.

DZIENNIK SYSTEMU INFORMATYCZNEGO
ŁZUK

L.p.	Data i godzina zdarzenia	Opis zdarzenia	Podjęte działania/wnioski	Podpis