# INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Podmiot: Pyrzyckie Przedsiębiorstwo Komunalne Sp. z o.o.

**ADRES: ul. Kościuszki 26, 74-200 Pyrzyce**

SPIS TREŚCI

## ROZDZIAŁ 1
## Postanowienia ogólne

### § 1

Celem Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych **zwanej dalej „Instrukcją”**, jest określenie zasad zapewniających bezpieczeństwo danym osobowym, które przetwarzane są za pomocą systemów informatycznych.

### § 2

1. Instrukcja jest jednym z elementów wewnętrznych polityk wdrożonych w podmiocie zgodnie z wymogami zawartymi w art. 24 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r w sprawie osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
2. Instrukcja ma zastosowanie do przetwarzania danych we wszystkich zbiorach danych, pod warunkiem, że do przetwarzania tych danych używane są systemy informatyczne.

### § 3

Przez użyte w Instrukcji określenia należy rozumieć:

1) **system informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
2) **zabezpieczenie systemu informatycznego** –zastosowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, mające na celu w szczególności zabezpieczenie danych przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, zmianą, utratą uszkodzeniem lub zniszczeniem;
3) **zbiór danych osobowych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentalizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
4) **przetwarzanie danych** – operacja lub zestaw operacji wykonanych na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
5) **usuwanie danych** – zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
6) **administrator** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych – Pyrzyckie Przedsiębiorstwo Komunalne Sp. z o.o., zwany dalej **PPK**;
7) **administrator systemu informatycznego (ASI)** – osoba wyznaczona przez administratora, nadzorująca przestrzeganie zasad ochrony danych przez użytkowników systemów informatycznych i odpowiadająca za odpowiednie zabezpieczenie danych osobowych przetwarzanych w systemach informatycznych;
8) **polityka** – Ogólna polityka ochrony danych osobowych wdrożona przez administratora;

9) **użytkownik** – rozumie się przez to osobę upoważnioną przez administratora do przetwarzania danych osobowych posiadającą uprawnienia do przetwarzania danych w systemach informatycznych;
10) **identyfikator użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
11) **hasło** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
12) **uwierzytelnianie** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
13) **nośniki danych osobowych** – dyskietki, laptopy, płyty CD lub DVD, pamięć flash, dyski twarde, taśmy magnetyczne lub inne urządzenia/materiały służące do przechowywania plików z danymi.

**§ 4**

1. Za ogólną kontrolę i nadzór nad przestrzeganiem postanowień niniejszej Instrukcji odpowiada administrator.
2. Administrator może wyznaczyć **Administratora systemu informatycznego** do poszczególnych lub wszystkich systemów informatycznych służących do przetwarzania danych osobowych. Wzór upoważnienia z opisem zakresu obowiązków stanowi **zał. nr 1** do niniejszej Instrukcji.
3. W przypadku braku powołania ASI administrator sam lub z pomocą wyspecjalizowanej firmy realizuje zadania związane ze stosowaniem zasad ochrony danych osobowych, w tym:
   1) sporządza kopie bezpieczeństwa dla baz sieciowych,
   2) pozbawia urządzenia i inne nośniki informacji przeznaczone do likwidacji zapisu danych lub – gdy nie jest to możliwe – uszkadza je trwale w sposób uniemożliwiający odczytanie danych,
   3) nadzoruje usuwanie awarii sprzętu komputerowego w sposób zapewniający bezpieczeństwo przetwarzanych danych osobowych,
   4) odpowiednio zabezpiecza dane osobowe wysyłane poza obszar przetwarzania danych określony w polityce,
   5) sprawuje nadzór nad czynnościami związanymi z ochroną przeciwwirusową i czynnościami serwisowymi dotyczącymi systemu informatycznego, w którym przetwarzane są dane osobowe,
   6) nadzoruje obieg i przetwarzanie wydruków z systemu informatycznego zawierających dane osobowe,
   7) podejmuje i nadzoruje wszelkie inne działania zmierzające do zapewnienia bezpieczeństwa przetwarzanych w systemie informatycznym danych osobowych.

## ROZDZIAŁ 2
## Zakres przedmiotowy Instrukcji

**§ 5**

Niniejsza Instrukcja zawiera w szczególności:
1. Ogólne informacje o systemach informatycznych wykorzystywanych w podmiocie do przetwarzania danych osobowych, w tym:

1) procedury rozpoczęcia, zawieszenia i zakończenia pracy,
2) sposób postępowania w zakresie komunikacji w sieci komputerowej,
3) metodę i częstotliwość sprawdzania obecności wirusów komputerowych oraz metodę ich usuwania;

2. Zasady dotyczące poszczególnych systemów informatycznych, w tym:
   1) sposób przydziału haseł dla użytkowników poszczególnych systemów i częstotliwości ich zmiany oraz wskazania osób odpowiedzialnych za te czynności,
   2) metody i częstotliwość tworzenia kopii awaryjnych,
   3) sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków,
   4) sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych.

**§ 6**

Działaniem Instrukcji objęci są wszyscy użytkownicy systemów informatycznych, w tym wyznaczony ASI.

**§ 7**

1. W przypadku stwierdzenia utraty lub kradzieży jakichkolwiek urządzeń lub oprogramowania komputerowego należy natychmiast poinformować ASI.
2. Ograniczanie przez PPK dostępu do zasobów systemów informatycznych przebiega w następujący sposób:
   1) fizyczny dostęp do sieci mogą mieć tylko takie urządzenia sieciowe, które uzyskały akceptację Administratora,
   2) logiczny dostęp do sieci – uzyskanie dostępu do zasobów sieciowych mogą mieć tylko zarejestrowani użytkownicy jednoznacznie zidentyfikowani,
   3) logowania się bezpośrednio na serwerach sieciowych,
   4) dostęp do aplikacji i baz danych – dostęp do aplikacji i baz danych wymaga uprzedniej identyfikacji i uwierzytelnienia użytkownika; przyznane użytkownikowi uprawnienia do korzystania z poszczególnych aplikacji i baz danych powinny być ograniczone wyłącznie do zakresu jego obowiązków służbowych.

## ROZDZIAŁ 3
## Nadawanie uprawnień do przetwarzania danych oraz ich rejestrowanie w systemie informatycznym

**§ 8**

1. Osobą odpowiedzialną za nadawanie uprawnień do przetwarzania danych w systemach informatycznych jest ASI.
2. Przyznanie lub cofnięcie uprawnienia dla użytkownika systemu nadawane jest przez firmę UNISOFT po uprzednim zgłoszeniu przez Kierownika działu, który kieruje wniosek najpierw do ASI, a ten następnie do firmy UNISOFT.
3. Firma zewnętrzna UNISOFT po nadaniu użytkownikowi identyfikatora do przetwarzania danych, musi niezwłocznie przekazać go ASI.
4. Każdy pracownik dopuszczony do przetwarzania danych w systemach informatycznych nadany ma oddzielny identyfikator.

5. Uprawnienia do przetwarzania danych ustają w momencie rozwiązania stosunku pracy z użytkownikiem danego konta, co skutkuje dezaktywacją konta w systemie informatycznym.
6. Na identyfikatorze może pracować jedynie użytkownik, któremu jest przypisany dany identyfikator. Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora i hasła dostępu innego użytkownika.
7. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych, informatyk niezwłocznie blokuje w systemie informatycznym służącym do przetwarzania danych osobowych oraz unieważnia przypisane mu hasło.
8. Kierownicy komórek organizacyjnych są zobowiązani informować ASI o zmianach w zakresie obowiązków podległych pracowników skutkujących koniecznością zmiany ich uprawnień.
9. Uprawnienia posiadane przez użytkownika nie mogą być rozszerzane, o ile nie istnieje umotywowana potrzeba związana ze zmianą zakresu obowiązków użytkownika.
10. W przypadku połączeń dokonywanych z sieci wewnętrznej uwierzytelnienie użytkownika polega na sprawdzeniu identyfikatora i hasła przypisanych do profilu użytkownika.
11. W przypadku połączeń zewnętrznych wymagane jest stosowanie tuneli VPN.
12. Jeżeli dany podsystem kontroli dostępu do systemów informatycznych nie funkcjonuje prawidłowo, uprawnienia użytkowników powinny być zablokowane. W przypadku nieprawidłowego funkcjonowania podsystemów kontroli dostępu, decyzje o dalszych działaniach podejmuje administrator.
13. W systemach informatycznych nie mogą być aktywne ogólnodostępne profile domyślne typu „gość”.
14. Osoby nie będące pracownikami PPK nie mogą uzyskać profilu użytkownika ani uprawnień w zakresie korzystania z systemów informatycznych bez uprzedniej, pisemnej zgody Administratora.

**§ 9**

1. Nazwa profilu użytkownika musi być unikatowa i nie powinna zmieniać się przez cały okres jego pracy w PPK, nie licząc przypadków takich jak np. zmiana nazwiska.
2. W celu jednoznacznego określenia użytkowników przyjmuje się następującą metodologię nadawania nazw kont: pierwsza litera imienia oraz nazwisko.
3. Identyfikator użytkownika powinien być inny dla każdego użytkownika, a po jego wyrejestrowaniu z systemu informatycznego, nie powinien być przydzielany innej osobie.

**§ 10**

1. Indywidualny zakres czynności osoby upoważnionej przy przetwarzaniu danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę tych danych przed:
   1) niepowołanym dostępem,
   2) nieuzasadnioną modyfikacją lub zniszczeniem,
   3) nielegalnym ujawnieniem,
   4) pozyskaniem – w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu danych osobowych.
2. Monitory komputerów powinny być tak ustawione, aby uniemożliwić osobom postronnym wgląd do danych osobowych.

## ROZDZIAŁ 4
## Procedury rozpoczęcia, zawieszenie i zakończenia pracy w systemie informatycznym

### § 11

1. Przed rozpoczęciem pracy w systemie informatycznym użytkownik zobowiązany jest do:
   1) zalogowania się do systemu z wykorzystaniem zastrzeżonych tylko dla siebie: identyfikatora i hasła w sposób uniemożliwiający ich ujawnienie osobom postronnym – hasło nie może zawierać mniej niż 8 znaków, osoba je tworząca obowiązana jest uczynić to w taki sposób, aby utrudnić jego ewentualne odczytanie, poprzez wprowadzenie do hasła: znaków szczególnych, cyfr, dużych liter itd.,
   2) sprawdzenia prawidłowości funkcjonowania sprzętu komputerowego i systemów, na swoim stanowisku pracy,
   3) w razie stwierdzenia nieprawidłowości, do powiadomienia o tym fakcie bezpośredniego przełożonego oraz osobę nadzorująca przypadku naruszeń,
   4) w razie stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub stanu wskazującego na istnienie takiej możliwości, do podjęcia odpowiednich kroków stosownie do zasad postępowania w sytuacji naruszenia zabezpieczenia danych osobowych.
2. Stanowiska pracy muszą być zablokowane lub wyłączone, gdy stanowisko nie jest używane.
3. Przerywając przetwarzanie danych użytkownik może zakończyć pracę w systemie informatycznym – wylogować się z systemu.
4. Po zakończeniu przetwarzania danych osobowych w danym dniu, osoba upoważniona zobowiązana jest do:
   1) zakończenie pracy w systemie informatycznym – wylogowanie się z systemu.
   2) wylogowania się z systemu informatycznego,
   3) wyłączenia sprzętu komputerowego oraz zamknięcia szaf, w których przechowuje się nośniki, na których utrwalone są dane osobowe,
   4) zamknięcia pomieszczeń.

## ROZDZIAŁ 5
## Kopie bezpieczeństwa

### § 12

Urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, powinny być zabezpieczone przed utratą tych danych wskutek awarii zasilania lub zakłóceń w sieci zasilającej. Zabezpieczenie to powinno być tak skonstruowane, by umożliwiało zapisanie danych we wszystkich uruchomionych aplikacjach i wykonanie kopii bezpieczeństwa.

### § 13

1. Ważne jest, żeby wszystkie istotne dane miały kopie zapasowe, dzięki czemu w przypadku uszkodzenia systemów komputerowych możliwe będzie odtworzenie danych i kontynuowanie działalności. Kopie zapasowe mają również stanowić gwarancję, że

okresowe problemy związane z systemem informatycznym nie będą miały wpływu na działalność operacyjną PPK i jej partnerów.
2. Procedury dotyczące wykonywania kopii bezpieczeństwa uwzględniają zarówno potrzeby PPK, jak i aktualny stan przepisów prawa.
3. Kopie bezpieczeństwa są wykonywane wg stałego harmonogramu - codziennie.
4. Tworzenie kopii bezpieczeństwa odbywa się poprzez automatyczny zapis pełnej kopii baz oraz przez ASI na zewnętrzny dysk twardy.
5. Tworzone kopie bezpieczeństwa powinny być opisane w sposób pozwalający na określenie ich zawartości.
6. Kopie bezpieczeństwa nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.
7. Kopie bezpieczeństwa powinny być przechowywane w sejfie lub w przypadku braku takiej możliwości w zamkniętych szafach, znajdujących się w pomieszczeniach, które również są zamykane na klucz.
8. Kopie bezpieczeństwa należy okresowo sprawdzać pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu oraz bezzwłocznie usuwać po ustaniu ich użyteczności.
9. Kopie bezpieczeństwa, które uległy uszkodzeniu lub stały się niepotrzebne pozbawia się zapisu danych w sposób uniemożliwiający ich odtworzenie.
10. Jeżeli pozbawienie zapisu nie jest możliwe, kopie są niszczone w sposób uniemożliwiający odczytanie bądź odtworzenie danych zawartych na nośniku kopii.
11. Dane mogą być odzyskiwane tylko i wyłącznie przez osoby upoważnione przez Administratora.
12. Użytkownicy komputerów przenośnych muszą zapewnić regularne wykonywanie kopii bezpieczeństwa przechowywanych przez nich danych.
13. Do celów archiwizacyjnych nie należy wykorzystywać mediów, które nie stanowią wiarygodnego sposobu przechowywania informacji.

## ROZDZIAŁ 6
## Sposób i czas przechowywania oraz zasady likwidacji nośników informacji

### § 14

1. Nośniki informatyczne, zawierające dane osobowe, przechowywane są na serwerze
2. Utworzone dodatkowe elektroniczne kopie zapasowe przechowywane są na dysku zewnętrznym.
3. Procedura przywracania danych w razie incydentu krytycznego – kopie zapasowe danych są wykonywane codziennie, a dane są zapisywane na dysku zewnętrznym. W sytuacji awarii powiadamiany jest Unisoft. W odpowiedzi na powiadomienie Unisoft podmienia dane.
4. Do miejsca przechowywania nośników informacji i kopii zapasowych dostęp mają tylko osoby upoważnione.
5. Z urządzeń, dysków lub innych nośników informatycznych, które zostały przeznaczone do przekazania innemu podmiotowi, usuwa się zapisane na nich dane.
6. Jedynie osoby upoważnione przez Administratora mogą zbywać lub utylizować wyposażenie komputerowe oraz nośniki informacji stanowiące własność PPK.
7. W przypadku tymczasowego (np. w celach serwisowych) lub trwałego (np. sprzedaż, darowizna) przekazywania osobom trzecim sprzętu komputerowego wszelkie wymienne nośniki danych powinny być usunięte. Jeśli jest to możliwe, również trwałe nośniki

danych powinny być usunięte. Jeśli nie jest to możliwe, usunięte powinny być dane zawarte na trwałych nośnikach. Do ich usunięcia powinny zostać użyte narzędzia zapewniające trwały i bezpieczny charakter tej operacji na przykład poprzez wielokrotne zapisanie całego obszaru nośnika losowymi danymi.

8. Nośniki wycofywane z użycia są przekazywane do zniszczenia. Ich zniszczenie musi mieć charakter trwały, uniemożliwiający odczytanie zawartych na nich informacji i powinno być nadzorowane przez ASI.
9. Procedura niszczenia nośników informacji:
   a) niszczeniu mogą podlegać następujące nośniki informacji: dysk twardy HDD lub SSD, pamięć USB, dysk twardy zewnętrzny, płyta CD.
   b) Dane z urządzenia (dyski twarde oraz pamięci USB) zostają zniszczone poprzez:
   - metodę niszczenia programowego tzn. sformatowanie oraz wielokrotne nadpisanie danych które mają gwarantować niemożliwość odtworzenia niszczonych danych,
   - metodę mechaniczną, tzn. sposób fizyczny poprzez wiercenie dziur w talerzach dysków lub uszkodzenie ich młotkiem.
   c) dane znajdujące się na płytach CD niszczone są w sposób fizyczny w przeznaczonej do tego niszczarce.
   d) Administrator zobowiązany jest do sporządzenia protokołu niszczenia nośników informacji, zgodnie z załącznikiem nr 3.

## ROZDZIAŁ 7
## Zabezpieczenie sprzętowe

### § 15

1. Ochrona antywirusowa jest realizowana poprzez zainstalowanie odpowiedniego oprogramowania antywirusowego.
2. System informatyczny podlega regularnej (co najmniej raz w tygodniu) kontroli pod kątem obecności wirusów komputerowych.
3. Wykryte zagrożenia usuwa się niezwłocznie z systemu informatycznego.
4. Przed przystąpieniem do unieszkodliwienia wirusa, należy zabezpieczyć dane zawarte w systemie przed ich utratą.
5. Oprogramowanie antywirusowe jest instalowane w miarę możliwości na wszystkich jednostkach komputerowych
6. Każdy użytkownik zobowiązany jest do korzystania z aktualnego oprogramowania antywirusowego na swoim komputerze. W zależności od możliwości technicznych powyższe oprogramowanie musi być aktywne przez cały czas działania komputera lub uruchamiane ręcznie na żądanie.
7. Osobą odpowiedzialną za powyższe działania jest ASI.
8. Program antywirusowy należy skonfigurować w sposób umożliwiający jego automatyczną aktualizację bez interwencji użytkownika. W przypadku gdy jest to niemożliwe, każdy użytkownik jest odpowiedzialny za aktualizację swojego oprogramowania antywirusowego dostarczanego przez wcześniej uzgodniony kanał dystrybucji lub na wezwanie ASI.
9. W przypadku wykrycia wirusa komputerowego, użytkownik systemu zobowiązany jest do natychmiastowego poinformowania o tym fakcie ASI.
10. Do czasu usunięcia wirusa lub otrzymania innych poleceń od ASI pracę na komputerze należy wstrzymać.

### § 16

1. Wszystkie kluczowe systemy informatyczne są zasilane przy pomocy wydzielonego systemu zasilania bezprzerwowego (UPS) i dodatkowo zabezpieczone przy użyciu urządzeń przeciwprzepięciowych. Deklarowana wydajność urządzeń UPS jest sprawdzana regularnie, nie rzadziej niż zgodnie z zaleceniami producenta.

## ROZDZIAŁ 8
## Konserwacja i naprawa systemu przetwarzającego dane osobowe

### § 17

1. Prace bieżące w dziedzinie konserwacji i naprawy systemu przetwarzającego dane osobowe prowadzi ASI lub w wypadku konieczności zaangażowania do w/w czynności innego specjalisty, są one wykonywane pod bezpośrednim nadzorem ASI
2. Naprawy i konserwacje są wykonywane wyłącznie przez upoważnionych pracowników lub zewnętrznych dostawców usług.
3. Urządzenia komputerowe, dyski twarde, lub inne informatyczne nośniki danych przeznaczone do naprawy, pozbawia się przed tymi czynnościami zapisu zgromadzonych na nich danych osobowych.
4. Dziennik konserwacji i napraw stanowi **zał. nr 2** do niniejszej Instrukcji.

## ROZDZIAŁ 9
## Zasady bezpiecznego korzystania z systemów informatycznych

### § 18

1. Wszelkie pliki zawierające kopie danych osobowych zawartych w systemie, wysyłanych poza system, muszą być zabezpieczone hasłem /szyfrowane/.
2. Nieuzasadnione kopiowanie danych z serwera na stacje robocze, bądź na nośniki informatyczne jest zabronione.

### § 19

1. Użytkownicy zobowiązani są do przestrzegania zasad ochrony antywirusowej.
2. Zabronione jest celowe opracowywanie, generowanie, kompilowanie, kopiowanie, rozpowszechnianie, uruchamianie lub próby wprowadzania kodów komputerowych, które:
   1) mają zdolność samo powielania się,
   2) mają zdolność uszkadzania lub innego utrudniania działalności pamięci komputerowej, plików systemowych lub oprogramowania,
   3) służą do omijania lub przełamywania zabezpieczeń i praw dostępu,
   4) wymagałyby wykorzystania większej ilości zasobów informatycznych, niż jest to niezbędne do zapewnienia prawidłowego działania systemów informatycznych PPK,
   5) powodowałyby zakłócenia w działaniu sieci informatycznej.
3. Systemy informatyczne razem z przechowywanymi na nich informacjami są narażone na szkody wyrządzane przez działanie niepożądanego oprogramowania. Z tego względu wszyscy użytkownicy powinni być świadomi zagrożeń związanych z działaniem niepożądanego oprogramowania. W celu wykrycia oraz zapobieżenia pojawiania się

niepożądanego oprogramowania wdrożone są odpowiednie mechanizmy kontrolne. W szczególności uwaga zwrócona jest na ochronę komputerów osobistych przed pojawianiem się wirusów komputerowych.
4. Zabezpieczenia przed niepożądanym oprogramowaniem opierają się na świadomości użytkowników, stosowaniu odpowiednich aplikacji zapobiegawczych oraz na prawidłowej kontroli dostępu do systemu.
5. Użytkownicy nie mogą samodzielnie instalować żadnego oprogramowania dostarczonego przez siebie lub osoby trzecie, niezależnie od sposobu, w jaki zostało nabyte. Na instalację oprogramowania, które nie jest niezbędne do zapewnienia działania systemów komputerowych każdorazowo musi wyrazić zgodę ASI w porozumieniu z Administratorem.
6. W czasie uruchamiania systemu operacyjnego komputera nie wolno zostawiać wymiennych nośników danych w napędach. Stacje robocze użytkowników są skonfigurowane tak, by system operacyjny był w pierwszej kolejności wczytywany z dysków twardych, a nie z wymiennych nośników danych.
7. Wszystkie media z danymi dostarczone z zewnątrz PPK nie mogą być użyte bez wcześniejszego sprawdzenia programem antywirusowym. Zabrania się wprowadzania danych nie dotyczących działalności PPK.
8. Wszystkie pliki przed wysłaniem lub przekazaniem stronom trzecim, tzn. osobom nie będącym pracownikami PPK, są testowane przez użytkowników komputerów oprogramowaniem antywirusowym.

## ROZDZIAŁ 10
## Postanowienia końcowe

### § 20

1. ASI zobowiązany jest do niezwłocznego podjęcia działań mających na celu powstrzymanie lub ograniczenie osobom niepowołanym dostępu do danych osobowych w szczególności przez:
   1) zmianę hasła dla użytkowników;
   2) fizyczne odłączenie urządzeń i tych segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie niepowołanej;
   3) wylogowanie użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych.
2. W przypadku uszkodzenia urządzeń służących do przetwarzania danych, utraty danych, lub ich zniekształcenia, odtwarza się bazy danych osobowych z ostatniej kopii bezpieczeństwa.
3. W sprawach nieuregulowanych niniejszą Instrukcją stosuje się przepisy prawa o ochronie danych osobowych.
4. Użytkownicy zobowiązani są do zapoznania się z niniejszą Instrukcją i do stosowania postanowień w niej zawartych przy przetwarzaniu danych osobowych w systemach informatycznych.
5. Naruszenie przez pracownika niniejszej Instrukcji może zostać potraktowane jako naruszenie obowiązków pracowniczych i powodować określoną przepisami Kodeksu Pracy odpowiedzialność pracownika.
6. Instrukcja jest dokumentem wewnętrznym i nie może być udostępniona osobom postronnym.
7. Integralną część dokumentacji stanowią załączniki:

Zał. nr 1 – Powołanie ASI
Zał. nr 2 – Protokół przeglądów informatycznych
Zał. nr 3 – Protokół zniszczenia nośnika informacji

**§ 21**

Niniejszy dokument wchodzi w życie z dniem 30-07-2019 roku.

Podpis:

…….....……
Administrator

załącznik nr 1

**Upoważnienie dla Administratora Systemów Informatycznych**

Administrator: ……..

dnia …… powołuje

Administratora systemów informatycznych: ……
i jednocześnie nadaje mu upoważnienie do przetwarzania danych w zbiorach danych osobowych prowadzonych przez administratora przetwarzanych za pomocą systemów informatycznych.
Upoważnienie jest ważne od chwili podpisania przez strony do dnia odwołania ASI przez administratora.

**ASI jest odpowiedzialny w szczególności za:**

1) nadzorowanie poprawności przetwarzania danych w systemach informatycznych,
2) bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
3) optymalizację wydajności systemu informatycznego, baz danych,
4) instalację i konfigurację sprzętu sieciowego i serwerowego,
   współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego,
5) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
6) zarządzanie kopiami awaryjnymi danych, w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
7) zarządzanie licencjami oraz procedurami ich dotyczącymi,
8) prowadzenie profilaktyki antywirusowej,
9) sprawowanie nadzoru nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
10) sprawowanie nadzoru nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, zlecanymi firmom.

**OŚWIADCZENIE ASI**

Oświadczam, że zapoznałem się z treścią i obowiązkami wynikającymi z tego upoważnienia oraz że jako Administrator systemów informatycznych będę nadzorował przestrzeganie zasad ochrony danych zgodnie z obowiązkami wynikającymi z zapisów wewnętrznych polityk dotyczących ochrony danych osobowych oraz przepisów prawa o ochronie danych osobowych.

Podpisy:

…… ……..
Administrator Administrator systemów informatycznych

załącznik nr 2

**Protokół przeglądów informatycznych**

| Lp. | Data przeglądu | Zakres przeglądu | Uwagi | Podpis wykonującego przegląd | Podpis ASI lub osoby upoważnionej |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Załącznik nr 3

**Protokół zniszczenia nośnika informacji**

Rodzaj nośnika informacji:
Dysk twardy HDD, SSD, pamięć USB, dysk twardy zewnętrzny, inne (właściwe podkreślić)

Producent i numer seryjny urządzenia:

……

Dane z urządzenia zostały zniszczone poprzez niszczenie programowe (sformatowanie oraz wielokrotne nadpisanie danych) oraz w sposób fizyczny metodą mechaniczną.

……..
Podpis osoby uprawnionej