# REGULAMIN

# OCHRONY DANYCH OSOBOWYCH

# W


14 listopada 2018 r

# SPIS TREŚCI

## DEFINICJE

Ilekroć w niniejszym regulaminie jest mowa o:

1. Administratorze danych – rozumie się przez to oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;. W niniejszej polityce bezpieczeństwa przez Administratora rozumie się Miejski Ośrodek Kultury w Lesznie, dalej zwaną „Administratorem".
2. Administratorze systemów informatycznych (lub „ASI") – rozumie się przez to osobę wyznaczoną przez Administratora, która odpowiada za zapewnienie sprawności, należytej konserwacji i wdrażania technicznych zabezpieczeń systemów informatycznych oraz odpowiada za to, aby systemy informatyczne, w których przetwarzane są dane osobowe spełniały wymagania przewidziane ustawą i rozporządzeniem.
3. Danych osobowych (lub „dane") – rozumie się informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
4. Inspektor Ochrony Danych (lub „IOD") – rozumie się osobę wyznaczoną przez Administratora na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań określonych w art. 39 RODO, między innymi:
    a) informowania administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
    b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty.
5. Osobie upoważnionej – rozumie się przez to osobę, która otrzymała od Administratora pisemne upoważnienie do przetwarzania danych.
6. Przetwarzaniu danych – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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.
7. Rozporządzeniu - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), określane również jako RODO.

8. Upoważnieniu – rozumie się przez to oświadczenie nadawane przez Administratora wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym oświadczeniu.
9. Zbiorze danych – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

## POSTANOWIENIA OGÓLNE

### § 1

W celu zapewnienia ochrony przetwarzanych danych osobowych zarówno za pomocą systemów informatycznych jak i w wersji papierowej Administrator wdrożył politykę bezpieczeństwa przetwarzania danych osobowych oraz instrukcję zarządzania systemem informatycznym RODO. Celem jak najlepszego zapoznania pracowników i współpracowników z zasadami ochrony danych osobowych wdraża się również niniejszy regulamin, na który składają się postanowienia zawarte w polityce bezpieczeństwa oraz instrukcji zarządzania, przydatne dla każdej osoby przetwarzającej dane podczas codziennego wykonywania obowiązków zawodowych.

## ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI I SYSTEMÓW INFORMATYCZNYCH

### § 2

1. Administrator może wyznaczyć inspektora ochrony danych, który jest odpowiedzialny za przetwarzanie danych zgodnie z ustawą oraz rozporządzeniem.
2. Administrator może wyznaczyć co najmniej jednego zastępcę IOD.
3. Zastępca IOD wykonuje wszystkie obowiązki należące do zakresu obowiązków IOD podczas jego nieobecności.

### § 3

Administrator może wyznaczyć Administratora Systemów Informatycznych.

### § 4

W przypadku niewyznaczenia IOD lub ASI za zapewnienie należytego przestrzegania zasad ochrony danych osobowych odpowiada Administrator.

### § 5

1. W przypadku powzięcia jakichkolwiek wątpliwości co do ewentualnej zgodności z prawem planowanych działań w zakresie przetwarzania danych, należy zwrócić się do IOD z wnioskiem o rozstrzygnięcie wątpliwości.
2. Przed udzieleniem przez IOD odpowiedzi w przedmiocie istniejących wątpliwości niedozwolone jest zbieranie danych osobowych i ich utrwalanie, a w przypadku posiadania już danych osobowych których wątpliwość dotycz należy, do czasu rozstrzygnięcia wątpliwości, wstrzymać wszystkie działania na danych osobowych, co do których istnieją wątpliwości czy są prawnie uzasadnione.

## OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

### § 6

1. Administrator obowiązany jest nadać upoważnienie do przetwarzania danych każdej osobie, która do przetwarzania danych będzie dopuszczona.
2. Upoważnienie do przetwarzania danych osobowych wygasa z chwilą upływu terminu wypowiedzenia lub rozwiązania umowy zawartej przez Administratora z osobą, której zostało nadane lub w przypadku gdy zostało nadane na czas określony z upływem czasu na jaki zostało nadane.
3. Osoba upoważniona przez Administratora nie ma prawa do nadawania dalszych upoważnień, chyba że upoważnienie do przetwarzania danych osobowych nadane przez Administratora zawiera upoważnienie do nadawania dalszych upoważnień.

### § 7

1. Każdy kto przetwarza dane osobowe obowiązany jest zachować w tajemnicy dane osobowe do których posiada dostęp zarówno zamierzony jak i przypadkowy, sposoby zabezpieczania danych jak również wszelkie informacje, które powzięły w czasie przetwarzania danych. Obowiązek zachowania danych w tajemnicy jest bezterminowy.
2. Podczas przetwarzania danych należy zachować szczególną ostrożność i podjąć wszelkie możliwe środki umożliwiające zabezpieczenie oraz ochronę danych przed nieuprawnionym dostępem, modyfikacją, zniszczeniem lub ujawnieniem.
3. Należy dochować należytej staranności podczas przesyłania dokumentów zawierających dane za pomocą środków komunikacji elektronicznej, w szczególności należy upewnić się, czy przesyłane za pomocą poczty elektronicznej dokumenty trafiły do właściwego odbiorcy.
4. W przypadku przesyłania za pomocą środków komunikacji elektronicznej zestawień, spisów czy innych dokumentów zawierających dane osobowe, przesyłany dokument należy zaszyfrować, a hasło przesłać w miarę możliwości innym środkiem komunikacji elektronicznej.

## OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH, NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

### § 8

1. Wszelkie dokumenty zwierające dane osobowe przechowywane są w szafach i pomieszczeniach zamykanych na klucz.
2. Osoba będąca dysponentem kluczy jest zobowiązana nie przekazywać kluczy do budynków i pomieszczeń w których przetwarzane są dane osobom nieuprawnionym, a ponadto obowiązana jest przedsięwziąć działania celem wykluczenia ryzyka ich utraty.
3. Osoba która utraciła posiadane klucze do pomieszczeń Administratora w których przetwarzane są dane, niezwłocznie zgłasza tą okoliczność Administratorowi.
4. Administrator podejmuje wszelkie niezbędne środki techniczne organizacyjne w celu zabezpieczenia pomieszczenia, do którego klucze utracono.

## ŚRODKI BEZPIECZEŃSTWA STOSOWANE PODCZAS PRACY Z DANYMI

### § 9

1. Osoba przetwarzająca dane po zakończeniu pracy porządkuje swoje stanowisko zabezpieczając dokumenty i nośniki elektroniczne z danymi w specjalnie do tego przeznaczonych szafach lub pomieszczeniach.
2. Niszczenie dokumentów zawierających dane odbywa się jedynie za pomocą niszczarki lub za pośrednictwem firmy zajmującej się niszczeniem dokumentów, po zawarciu umowy o powierzeniu przetwarzania danych osobowych.
3. Każdy dokument zawierający dane, a nieużyteczny niszczy się niezwłocznie.
4. Podczas korzystania z urządzeń wielofunkcyjnych należy zachować szczególną ostrożność. Dokumenty kopiowane bądź skanowane wyjmowane są z urządzenia wielofunkcyjnego niezwłocznie po ich użyciu. Dotyczy to również dokumentów powstałych na skutek kopiowania bądź skanowania.
5. Przebywanie osób trzecich w obszarze, w którym przetwarzane są dane jest dopuszczalne za zgodą Administratora lub w obecności osoby upoważnionej.

## POSTĘPOWANIE W RAZIE ZAISTNIENIA ZAGROŻENIA DLA BEZPIECZEŃSTWA PRZETWARZANYCH DANYCH OSOBOWYCH LUB NARUSZENIA ZASAD PRZETWARZANIA DANYCH OSOBOWYCH

### § 10

1. W przypadku podejrzenia naruszenia zasad bezpieczeństwa danych osobowych lub naruszenia zabezpieczeń stosowanych przez Administratora dla ochrony przetwarzanych danych osobowych należy niezwłocznie zawiadomić IOD, jeżeli jest wyznaczony. Jeżeli IOD nie został wyznaczony należy niezwłocznie zawiadomić Administratora o dostrzeżonych lub podejrzewanych naruszeniach.
2. W przypadku opisanym w ust. 1 IOD przeprowadza sprawdzenie doraźne. Sprawdzenie jest dokonywane niezwłocznie.
3. Przy dokonywaniu sprawdzenia IOD przysługują uprawnienia wskazane w rozporządzeniu ministra administracji i cyfryzacji w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji z dnia 11 maja 2015 r. (Dz.U. z 2015 r. poz. 745), w szczególności prawo:
   1) utrwalenia danych z systemu informatycznego służącego do przetwarzania lub zabezpieczania na informatycznym nośniku danych lub dokonania wydruku tych danych;
   2) odebrania wyjaśnień osoby, której czynności objęto sprawdzeniem;
   3) sporządzeniu kopii otrzymanego dokumentu;
   4) sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych.
4. Jeżeli IOD nie został wyznaczony Administrator w przypadku o którym mowa w ust. 1 obowiązany jest przeprowadzić postepowanie wyjaśniające i ustalające skutki oraz przyczyny naruszenia lub narażenia na naruszenie zasad bezpieczeństwa i sposobów zabezpieczenia, w sposób odpowiadający czynnościom podejmowanym przez IOD w przypadku sprawdzenia doraźnego.

## PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

### § 11

Użytkownikowi systemu informatycznego zostaje nadany dostęp po:

1) Zapoznaniu z przepisami dotyczącymi ochrony danych osobowych.
2) Podpisaniu oświadczenia o zapoznaniu się z niniejszą dokumentacją przetwarzania danych osobowych.
3) Podpisaniu oświadczenia o zachowaniu informacji (w tym danych osobowych), do których użytkownik będzie miał dostęp podczas wykonywania obowiązków służbowych lub zobowiązań umownych oraz środków ich zabezpieczania w tajemnicy (również po ustaniu łączącej strony umowy), w tym powstrzymanie się od wykorzystywania ich w celach pozasłużbowych.
4) Otrzymaniu upoważnienia do przetwarzania danych osobowych.

## POLITYKA HASEŁ

### § 12

1. Każdy użytkownik systemu informatycznego musi posiadać unikalny identyfikator i wprowadzone przez siebie hasło autoryzujące jego osobę w systemie informatycznym.
2. Hasła użytkowników lub inne dane uwierzytelniające podlegają szczególnej ochronie.
3. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła (prócz pierwszego hasła do systemu nadawanego przez administratora systemu informatycznego) i jego przechowywanie.
4. Każdy użytkownik posiadający dostęp do systemów informatycznego administratora danych jest obowiązany do:
    1) zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystanych do pracy w systemie informatycznym;
    2) niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia;
    3) niezwłocznej zmiany hasła tymczasowego, przekazanego przez administratora systemu informatycznego;
    4) poinformowania administratora systemu informatycznego oraz administratora bezpieczeństwa informacji o podejrzeniu lub rzeczywistym ujawnieniu hasła;
    5) stosowania haseł o minimalnej długości 8 znaków, zawierających kombinację małych i dużych liter oraz cyfr i/lub znaków specjalnych;
    6) stosowania haseł nie posiadających w swojej strukturze części loginu;
    7) stosowania haseł nie będących zbliżone do poprzednich (np.Tadeusz$2013 - Tadeusz$2014);
    8) zmiany wykorzystywanych haseł nie rzadziej niż raz na 30 dni.
5. Hasła zachowują swoją poufność również po ustaniu ich użyteczności.
6. Zabronione jest:
    1) zapisywanie haseł w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób;

2) stosowanie haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.;

3) używanie tych samych haseł w różnych systemach operacyjnych i aplikacjach;

4) udostępnianie haseł innym użytkownikom;

5) przeprowadzanie prób łamania haseł;

6) wpisywanie haseł „na stałe" (np. w skryptach logowania) oraz wykorzystywania opcji autozapamiętywania haseł (np. w przeglądarkach internetowych);

7) po trzykrotnym, błędnym wprowadzeniu hasła użytkownik jest zobowiązany zgłosić ten fakt do administratora systemu informatycznego, w celu zresetowania hasła dostępowego.

## ZASADY POSTĘPOWANIA Z KLUCZAMI KRYPTOGRAFICZNYMI

### § 13

1. W systemach obsługujących transmisję danych osobowych wrażliwych lub informacji poufnych administratora danych powinny być wykorzystywane klucze kryptograficzne służące do zabezpieczenia danych.
2. Przekazywanie kluczy użytkownikom powinno odbywać się w sposób protokolarny, o ile nie następuje w drodze teletransmisji.
3. Obowiązkiem użytkownika jest zabezpieczenie kluczy (prywatnych) przed dostępem osób nieupoważnionych.
4. W przypadku stwierdzenia ujawnienia klucza osobie nieupoważnionej lub podejrzenia o jego ujawnienie należy bezzwłocznie powiadomić administratora systemu informatycznego oraz administratora bezpieczeństwa informacji.
5. Dane osobowe wrażliwe lub informacje poufne administratora danych, do których nie stosuje się kluczy kryptograficznych, można przesyłać wyłącznie pocztą elektroniczną po uaktywnieniu funkcji podpisywania i szyfrowania pliku.
6. Każdy użytkownik korzystający z kluczy kryptograficznych jest zobowiązany do ich użytkowania i przechowywania w sposób uniemożliwiający utratę lub dostęp osób niepowołanych.
7. W przypadku podejrzenia lub rzeczywistego naruszenia bezpieczeństwa klucza fakt ten należy niezwłocznie zgłosić administratorowi systemu informatycznego oraz administratorowi bezpieczeństwa informacji.

## PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA, PROWADZENIA I ZAKOŃCZENIA PRACY W SYSTEMIE INFORMATYCZNYM

### § 14

1. Rozpoczęcie pracy w systemie informatycznym następuje po wprowadzeniu unikalnego identyfikatora i hasła.
2. Zawieszenie pracy w systemie informatycznym tj. brak wykonywania jakichkolwiek czynności przez okres 5 minut w systemie informatycznym powoduje automatycznie uruchomienie systemowego wygaszacza ekranu blokowanego hasłem. Zastosowanie powyższego mechanizmu nie zwalnia użytkownika z obowiązku każdorazowego blokowania ekranu wygaszaczem chronionym hasłem po odejściu od stanowiska.

3. W sytuacji gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlaną treść.
4. Przed zakończeniem pracy należy upewnić się czy dane zostały zapisane, aby uniknąć ich utraty danych.
5. Po zakończeniu pracy, użytkownik obowiązany jest wylogować się z systemu informatycznego przetwarzającego dane osobowe i z systemu operacyjnego, zabezpieczyć nośniki informacji (elektroniczne i papierowe) oraz wyłączyć komputer.
6. Użytkownik systemu informatycznego przetwarzającego dane osobowe niezwłocznie powiadamia administratora systemu w przypadku, gdy:
    1) Wygląd systemu, sposób jego działania, zakres danych lub sposób ich przedstawienia przez system informatyczny odbiega od standardowego stanu uznawanego za typowy dla danego systemu informatycznego;
    2) Niektóre opcje, dostępne użytkownikowi w normalnej sytuacji, przestały być dostępne lub też opcje niedostępne użytkownikowi w normalnej sytuacji, stały się dostępne.

## ZASADY KORZYSTANIA ZE SŁUŻBOWEJ POCZTY ELEKTRONICZNEJ

### § 15

1. Użytkownikowi zostaje nadany dedykowany adres skrzynki poczty elektronicznej działający w domenie administratora danych.
2. Informacja o służbowym adresie skrzynki pocztowej jest jawna i dostępna powszechnie, w tym może być dostępna na łamach witryny internetowej administratora danych w postaci książki adresowej.
3. Nadany użytkownikowi adres skrzynki poczty elektronicznej służy wyłącznie do realizacji celów służbowych lub umownych. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów informatycznych administratora danych podlega rejestrowaniu i może być monitorowana. Informacje przesyłane za pośrednictwem sieci administratora danych (w tym do i z Internetu) nie stanowią własności prywatnej użytkownika.
4. Wszelka korespondencja elektroniczna prowadzona przez pracownika, a niezwiązana z działalnością administratora danych, powinna być prowadzona przez prywatną skrzynkę poczty elektronicznej użytkownika.
5. Użytkownicy mają prawo korzystać z systemu poczty elektronicznej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
6. Korzystanie z systemu poczty elektronicznej dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych lub umownych, a także na wydajność systemu poczty elektronicznej.
7. Zabronione jest:
    1) wysyłanie materiałów służbowych na konta prywatne (np. celem pracy nad dokumentami w domu);
    2) wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić wizerunkowi administratora danych;
    3) odbieranie przesyłek z nieznanych źródeł;

4) otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.;

5) przesyłanie pocztą elektroniczną plików wykonywalnych typu: bat, com, exe, plików multimedialnych oraz plików graficznych;

6) ukrywanie lub dokonywanie zmian tożsamości nadawcy;

7) czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika;

8) odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem; w przypadku otrzymania takiej wiadomości należy przesłać ją administratorowi systemu informatycznego;

9) posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy lub obowiązków umownych;

10) wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb administratora danych lub do poszukiwania dodatkowego zatrudnienia.

## ZASADY KORZYSTANIA Z SIECI PUBLICZNEJ (INTERNET)

### § 16

1. Zdalne Korzystanie z systemów informatycznych poprzez sieć publiczną może mieć miejsce po zastosowaniu systemu uwierzytelniania użytkownika i szyfrowanego kanału transmisji.
2. Zdalny dostęp do serwerów w celach administracyjnych może mieć miejsce po zastosowaniu systemu uwierzytelniania użytkownika i szyfrowanego kanału transmisji.
3. Dostęp użytkowników do sieci publiczne (Internet) powinien być ograniczony do niezbędnego minimum na danym stanowisku pracy.
4. Wprowadza się całkowite ograniczenia w dostępie do treści uznanych za pornograficzne, rasistowskie, traktujące o przemocy, przestępstwach, jak również do protokołów umożliwiających wymianę plików w sieciach z naruszeniem przepisów prawa.

## ZASADY POSTĘPOWANIA Z NOŚNIKAMI ELEKTRONICZNYMI ORAZ VPN PODCZAS PRACY POZA OBSZAREM PRZETWARZANIA DANYCH

### § 17

1. Każdy użytkownik wymiennych nośników elektronicznych oraz użytkownicy zdalnych dostępów do sieci służbowej administratora danych (VPN) oraz użytkownicy elektronicznych kart dostępu ponoszą całkowitą odpowiedzialność za powierzony do użytkowania sprzęt oraz są obowiązani do stosowania się do poniższych zasad:
   1) Zabrania się pozostawiania bez opieki w miejscach publicznych nośników wymiennych przetwarzających informacje administratora danych.
   2) Komputery przenośne należy przewozić jako bagaż podręczny i w miarę możliwości je maskować.
   3) Użytkownik wykonując czynności zawodowe lub umowne w domu powinien zadbać

o należyte zabezpieczenie powierzonego sprzętu oraz dostępu do informacji przed nieautoryzowanym dostępem osób trzecich.

4) Zabrania się spożywania posiłków i picia podczas pracy z powierzonym sprzętem.

5) Zabrania się udostępniania osobom trzecim nośników elektronicznych informacji oraz powierzonego sprzętu będącego własnością spółki.

6) W przypadku utraty nośnika elektronicznego lub sprzętu komputerowego należy ten fakt bezzwłocznie zgłosić do bezpośredniego przełożonego lub administratora systemu informatycznego. Bezpośredni przełożony lub administrator systemu informatycznego bezzwłocznie zgłaszają taki fakt do administratora bezpieczeństwa informacji, ponieważ zagubienie nośnika przetwarzającego dane może wiązać się z utratą poufności informacji chronionych przez administratora danych.

7) Problemy wynikające z nieprawidłowego funkcjonowania sprzętu komputerowego należy zgłaszać administratorowi systemu informatycznego.

## UŻYTKOWANIE SPRZĘTU KOMPUTEROWEGO, OPROGRAMOWANIA, NOŚNIKÓW DANYCH

### § 18

1. Do sprzętu komputerowego zalicza się między innymi:
   1) komputery stacjonarne,
   2) komputery przenośne,
   3) tablety,
   4) smartphony,
   5) drukarki,
   6) modemy,
   7) monitory,
   8) routery,
   9) osprzęt dostarczony razem z wyżej wymienionym sprzętem lub zakupiony oddzielnie, a w szczególności: zasilacze, torby, klawiatury, myszki komputerowe.
2. Administrator udziela pomocy użytkownikowi w obsłudze sprzętu i oprogramowania.
3. W przypadku niepoprawnego i niezgodnego z przeznaczeniem użytkowania przez użytkownika sprzętu komputerowego, administrator systemu informatycznego informuje o powyższym administratora bezpieczeństwa informacji.
4. Użytkownik jest zobowiązany do dbałości o sprzęt oraz oprogramowanie, a także odpowiedzialny za zabezpieczenie go przed używaniem przez osoby nieuprawnione oraz do ochrony przed kradzieżą lub zagubieniem.
5. Użytkownik nie może samodzielnie zmieniać konfiguracji przekazanego sprzętu komputerowego oraz instalować, usuwać oprogramowania., w tym nie może używać na przekazanym sprzęcie prywatnego oprogramowania.

## KORZYSTANIE Z URZĄDZEŃ KOMUNIKACJI GŁOSOWEJ, FAKSOWEJ I WIZYJNEJ

### § 19

1. Każdy użytkownik zobowiązany jest do przestrzegania zakazu prowadzenia rozmów, podczas których może dochodzić do wymiany informacji danych osobowych lub informacji poufnych u administratora danych, jeśli rozmowy te odbywają się w miejscach publicznych, otwartych pomieszczeniach biurowych lub takich, które nie gwarantują zachowania poufności rozmów.
2. Odczytanie wiadomości z faksów, automatycznych sekretarek lub systemów poczty głosowej powinno być możliwe wyłącznie po wprowadzeniu indywidualnego hasła. W przypadku braku takiej możliwości urządzenia należy zabezpieczyć przed dostępem osób nieuprawnionych.
3. Zabronione jest wykorzystywanie domyślnych („fabrycznych") haseł dla ww. urządzeń.
4. Przekazywanie za pomocą urządzeń faksowych dokumentów zawierających dane osobowe wrażliwe lub informacje poufne u administratora danych jest zabronione.
5. Drukarki nie mogą być pozostawione bez kontroli, jeśli są wykorzystywane (lub wkrótce będą) do drukowania dokumentów zawierających informacje wrażliwe.

## OCHRONA PRZED SZKODLIWYM OPROGRAMOWANIEM

### § 20

1. Zidentyfikowanymi obszarami systemu informatycznego administratora danych narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania są dyski twarde lub karty pamięci urządzeń, pamięć RAM oraz elektroniczne nośniki informacji.
2. Drogą przedostania się wirusów lub szkodliwego oprogramowania może być sieć publiczna, wewnętrzna sieć teleinformatyczna lub elektroniczne nośniki informacji.
3. Użytkownicy systemu mają obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.
4. W przypadku stwierdzenia pojawienia się wirusa i braku możliwości usunięcia go przez program antywirusowy, użytkownik powinien skontaktować się z administratorem systemu informatycznego.

## POSTANOWIENIA KOŃCOWE

### § 21

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.
2. W sprawach nieuregulowanych w regulaminie lub polityce bezpieczeństwa mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy ustawy.