# INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI

Instrukcja Zarządzania Systemem Informatycznym zwana dalej „Instrukcją" jest integralną częścią Polityki Bezpieczeństwa obowiązującej w PTBSie w Pszczynie. Instrukcja obejmuję przede wszystkim:

1. praktyki nadawania uprawnień do przetwarzania danych, ich rejestrowania w systemie informatycznym oraz określenie osoby odpowiedzialnej za te czynności,
2. metody rejestrowania i wyrejestrowywania użytkowników oraz wskazania osób odpowiedzialnych za te czynności,
3. procedury rozpoczęcia, zawieszenia i zakończenia pracy,
4. częstotliwość oraz metody tworzenia kopii awaryjnych,
5. metody sprawdzania obecności wirusów w komputerach, ich usuwania oraz określenie czasookresu tych czynności,
6. określenie czas i sposobu przechowywania nośników informacji, w tym m. in. kopii informatycznych i wydruków,
7. monitorowanie i konserwacja systemu oraz zbioru danych osobowych,
8. postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego.

Administratorem Danych Osobowych zawartych i przetwarzanych w systemach informatycznych PTBSu jest Zarząd Spółki.

Instrukcja ma zastosowanie do każdego obszaru danych osobowych, który jest przetwarzany w systemach informatycznych Spółki lub zapisany jest w formie elektronicznej na nośnikach zewnętrznych.

Głównymi zagrożeniami, które będą miały wpływ dla poprawnego funkcjonowania systemów informatycznych związane są z awaryjnością sprzętu komputerowego, oprogramowania, czynnika ludzkiego oraz zdarzeń losowych.

W celu wprowadzenia odpowiednich zabezpieczeń zarówno technicznych jak i organizacyjnych Administrator winien przeprowadzić ocenę ryzyka, który obejmuje analizę zagrożeń, podatności, skutków wystąpienia zagrożeń oraz istniejących zabezpieczeń.

## I. Procedura nadawania uprawnień do przetwarzania danych oraz procedury rejestracji tych uprawnień w systemie informatycznym oraz wyznaczenie osoby odpowiedzialnej za te czynności.

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych ma obowiązek zapoznać się z:

a) rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119, s. 1) (dalej: RODO) oraz),

b) polityką bezpieczeństwa przy przetwarzaniu danych osobowych w PTBS;

c) niniejszą instrukcją.

2. Wzór nadawania i zmiany uprawnień do przetwarzania danych osobowych w PTBS określono w **załączniku nr 9** do Polityki Bezpieczeństwa.

3. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po:

a) podaniu identyfikatora użytkownika i właściwego hasła w przypadku obsługi programu Mieszczanin, Płatnik, stron internetowych, Urzędu Skarbowego, Zakładu Ubezpieczeń Społecznych, EPUAPu, KRSu, Banki,

b) podaniu właściwego hasła dostępu do stanowiska komputerowego.

4. Dostęp do danych na serwerze posiadają jedynie upoważnieni pracownicy przypisani do tzw. „grupy roboczej”.

5. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.

6. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.

7. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą, jako naruszenie podstawowych obowiązków pracowniczych.

8. Pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia.

9. Odebranie uprawnień pracownikowi następuje przez Administratora Danych Osobowych z podaniem daty oraz przyczyny odebrania uprawnień.

## II. Metody i środki uwierzytelniania (polityka haseł)

1. Dane osobowe przetwarzana są z użyciem dedykowanych serwerów, komputerów stacjonarnych.
2. Przy wyborze hasła obowiązują następujące zasady:
1) minimalna długość hasła - 8 znaków;
2) zakazuje się stosować:
a) swojej nazwy użytkownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę, itp.),
b) swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie,
c) imion (w szczególności imion osób z najbliższej rodziny),
d) ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy, na której mieszka lub pracuje, itp.,
e) przewidywalnych sekwencji znaków z klawiatury np.: QWERTY", "12345678", itp.,
f) identyfikatorem użytkownika;
3) należy stosować:
a) hasła zawierające kombinacje liter i cyfr,
b) hasła zawierające znaki specjalne: znaki interpunkcyjne, nawiasy, symbole @, #, &, itp., o ile system informatyczny na to pozwala,
c) hasła łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim.
3. Hasła wpisywane z klawiatury nie mogą pojawiać się na ekranie monitorów w formie jawnej.
4. W przypadku gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest do natychmiastowej zmiany hasła lub w razie problemów powiadomić o tym fakcie Administratora Danych Osobowych.
5. Zaleca się wprowadzenia w poszczególnych programach, na których pracują wszyscy pracownicy cykliczne wymuszanie zmiany hasła co 60 dni. W archiwum komputera pozostaje w pamięci 10 ostatnich wprowadzonych haseł (kopie przechowuje serwer), dlatego każde następne musi być różne od nich. W przypadku wprowadzenia pięciu niepoprawnych haseł konto użytkownika blokuje się na 10 minut. Taka blokada może zaistnieć 2 razy, zaś po

kolejnych próbach wejścia do systemu i ponownym wprowadzeniu błędnego hasła następuję blokada całkowita. Wówczas tylko operator może zresetować hasło.

## III. Procedura rozpoczęcia, zawieszenia i zakończenia pracy przeznaczona dla użytkowników systemu informatycznego służącego do przetwarzania danych osobowych.

1. Dane osobowe których administratorem jest PTBS mogą być przetwarzane w sposób tradycyjny lub z użyciem systemu informatycznego jedynie na potrzeby realizowana zadań statutowych i organizacyjnych PTBS.
2. Rozpoczęcie pracy użytkownika w systemie informatycznym następuje po poprawnym uwierzytelnieniu (zalogowaniu).
3. Rozpoczęcie pracy w aplikacji musi być przeprowadzone zgodnie z instrukcją zawartą w dokumentacji aplikacji.
4. W przypadku braku aktywności użytkownika na stanowisku komputerowym przez czas dłuższy niż 10 minut, stanowisko zostaje automatycznie zablokowane przez uaktywnienie wygaszacza ekranu. Wznowienie pracy następuje po poprawnym uwierzytelnieniu.
5. Wydruki zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym ich odczytanie przez osoby postronne. Wydruki nieprzydane należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.
6. Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać, na czas nieobecności osób zatrudnionych, w sposób uniemożliwiający dostęp do nich osobom trzecim.
7. Użytkownik niezwłocznie powiadamia Administratora Danych Osobowych w przypadku podejrzenia fizycznej ingerencji w przetwarzane dane osobowe lub użytkowane narzecza programowe lub sprzętowe. Wówczas, użytkownik jest zobowiązane do natychmiastowego wyłączenia sprzętu.
8. W przypadku nieobecności pracownika, dopuszcza się dostęp do stanowiska komputerowego przez zalogowanie użytkownika „Administrator". Hasło dostępu dla użytkownika „Administrator" jest znane Administratorowi Danych Osobowych.
9. W Spółce powstał obecnie dysk wspólny zasobów (share data), który jest podzielony na katalogi działowe. Każdy z tych katalogów ma przypisane dwa uprawnienia: do odczytu oraz odczytu i zapisu. Przynależność do folderu jest przypisana do pracowników pełniących określone funkcje. Wyjątek stanowi katalog „wymiana", do którego dostęp mają wszyscy

pracownicy z dostępem odczytu i zapisu. Dysk ten jest wykorzystywany przy zastępstwach za pracowników.

## IV. Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

1. Zbiory danych osobowych w systemie informatycznym są zabezpieczane przed utratą lub uszkodzeniem za pomocą:
   - urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej,
   - sporządzanie kopii zapasowych (kopie pełne/narastające).

2. Pełne kopie zapasowe zbiorów danych tworzone są cyklicznie. Są to kopie przyrostowe
- kopie z pulpitów robione są codziennie,
- kopie serwerów trafiają do chmury (oddzielna lokalizacja).

3. W szczególnych sytuacjach np. przed aktualizacją/zmianą oprogramowania lub zmianą systemu należy wykonać bezwzględnie pełną kopię zapasową systemu.

4. Nośniki danych po ustaniu ich użyteczności należy pozbawić danych lub zniszczyć w sposób uniemożliwiający odczyt danych.

5. Kopie wykonuje się:
- od poniedziałku do piątku o godzinie 21:00 (kopia całego serwera w postaci zaszyfrowanej). Wykonywana jest tez 1 kopia roczna (8 kopii tygodniowo w tym 30 kopii dziennych)
- kopia codzienna o godzinie 22:00 (8 kopii tygodniowych i 21 dziennych).

6. Podział serwera w Spółce:
a). serwer bazodanowy i aplikacji
b). serwer tożsamościowy połączony z serwerem plikowym.

## V. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

1. Przeglądy i konserwacje systemu oraz zbiorów danych wykonuje Administrator Danych Osobowych na bieżąco.
2. Naprawy i przeglądów sprzętu komputerowego użytkowanego w systemie może dokonywać wyspecjalizowana firma informatyczna, której kompetencje nie budzą

wątpliwości, co do wykonania usługi. Z firmą tą jest obowiązek podpisania umowy powierzenia przed przystąpieniem do prac.

3. W przypadku konieczności naprawy poza miejscem użytkowania, sprzęt komputerowy, przed oddaniem do serwisu, powinien być odpowiednio przygotowany. Dane należy zarchiwizować na nośniki informacji.
4. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji, może być dokonana tylko za wiedzą i zgoda Administratora Danych Osobowych.

## VI. Utylizacja elektronicznych nośników

1. Urządzenia, dyski i inne elektroniczne nośniki danych, zawierające dane osobowe, a przeznaczone do likwidacji – pozbawia się skutecznie zapisu tych danych, a gdy jest to niemożliwe, należy uszkodzić nośnik tak, aby nie było możliwe ich odczytanie.
2. Dokumentacja papierowa niszczona jest w niszczarkach paskowych oraz tam, gdzie to wymagane w niszczarkach o podwyższonym standardzie.
3. Dokumentacja papierowa może być niszczona za pośrednictwem firmy niszczącej dokumenty. Firma zobowiązana jest do wykazania się bezpieczną procedurą utylizacji (np. posiadać certyfikat ISO27001, nagrania z procesu transportu i utylizacji itp.)

## VII. Wydruki

1. Dokumenty papierowe, na których znajdują się dane osobowe, są przechowywane w zamykanych na klucz szafach.
2. Wydruki zawierające dane osobowe przeznaczone do usunięcia niszczy się w niszczarce, natomiast inne przechowywane są w warunkach uniemożliwiających dostęp do nich osób nieupoważnionych**.**

## VIII. Zabezpieczenia systemu informatycznego

### 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.

Dopuszcza się możliwość przyłączenia sieci internetowej do systemu, w którym przetwarzane są dane osobowe z zachowaniem następujących warunków:
a) na każdym komputerze musi być zainstalowane oprogramowanie antywirusowe (eset not antywirus),
b) każdy e-mail wpływający do PTBS musi zostać sprawdzony pod kątem wstępowania wirusów,
c) aktualizacje programów antywirusowych są dokonywane automatycznie:
- w każdy poniedziałek o godzinie 12:00 wykonywane jest pełne skanowanie systemu,
- w trybie ciągłym aktualizacja stron/miejsc przeglądanych,
d) zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym, którego dokonuje użytkownik zamierzający go użyć,
e) zabrania się odbierania z Internetu plików niewiadomego pochodzenia oraz odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym.
2. Cykliczne kontrole antywirusowe na wszystkich komputerach systemu przeprowadzane są automatycznie. Raport z kontroli będzie robiony raz w roku i przechowywany w formie elektronicznej i/lub papierowej przez Administratora Danych Osobowych.
3. Użytkownicy systemu są odpowiedzialni za nieudostępnianie stanowisk pracy osobom trzecim.

**ZABEZPIECZENIA INFRASTRUKTURY IT I APLIKACJI**

1. Zakazuje się samowolnego instalowania oprogramowania. Instalacji oprogramowania może dokonać tylko firma zewnętrzna świadcząca usługi informatyczne na podstawie zgody Administratora.
2. Na stacjach roboczych zastosowano „zahasłowane wygaszacze ekranu”, aktywowane po 10 minutach nieaktywności użytkownika.
3. Ustawienie monitorów uniemożliwia wgląd w dane przez osoby postronne. W przypadku gdy nie ma możliwości ustawienia monitorów w ten sposób zakładane są folie (filtry, osłony) ochronne na ekrany.
4. Dla aplikacji webowych stosowane jest szyfrowanie połączeń internetowych z użyciem protokołu SSL.

## ZABEZPIECZENIA KOMPUTERÓW PRZENOŚNYCH

1. Komputery przenośne (laptopy) powinny być zabezpieczone przed dostępem osób nieuprawnionych. Obecnie w Spółce jest 1 laptop.
2. Zabezpieczenie komputera powinno być zrealizowane przez wymaganie hasła dostępu, wprowadzane podczas uruchamiania komputera.
3. Nie dopuszcza się używania komputera do połączeń z siecią publiczną przez niezabezpieczone połączenia sieciowe, lub co do których istnieje podejrzenie, że połączenie może być niezabezpieczone. W Spółce działa siec zamknięta
4. Nie dopuszcza się używania komputerów przenośnych przez inne osoby niż te, którym zostały powierzone lub zostały upoważnione przez Administratora Danych.
5. Osoby, którym komputery przenośne zostały powierzone mają obowiązek ich zabezpieczenia przed kradzieżą, zgubieniem, dostępem osób nieupoważnionych, zniszczeniem, uszkodzeniem.
6. Jeżeli na dysku komputera przenośnego są zapisywane pliki lub bazy danych zawierające dane osobowe, dysk komputera powinien być szyfrowany.

## IX. Procedura wykonywania napraw i konserwacji

1. Administrator lub firma zewnętrzna świadcząca usługi informatyczne odpowiada za sprawdzanie poprawności działania systemów informatycznych, w tym: stacji roboczych, serwerów, drukarek, baz danych, aplikacji, poczty email.
2. Administrator lub Informatyk odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia.
3. W przypadku napraw dokonywanych na zewnątrz z komputerów należy uprzednio wymontować dyski i wszelkie nośniki zawierające dane osobowe.
4. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest zawarcie specjalnego zapisu w umowie serwisowej, gwarantującego poufność i bezpieczeństwo naprawy (należy na to zwrócić uwagę przy zakupach sprzętu oraz podpisywaniu umów serwisowych).
5. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest przekazywanie do naprawy uszkodzonego sprzętu z danymi zaszyfrowanymi na dysku / karcie pamięci. Sprzęt przekazywany jest do serwisu bez podania hasła.

6. Rekomendowane jest korzystanie z serwisu, który dokonuje napraw u klienta (umowy gwarancyjne on-site).
7. Czynności konserwacyjne i naprawcze wykonywane przez osoby nieposiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych) muszą być wykonywane pod nadzorem osób upoważnionych.
8. 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.
9. Dopuszczalne jest zdalne prowadzenie prac serwisowych przez upoważnionego serwisanta. Zdalne prowadzenie prac odbywa się na żądanie Administratora lub z inicjatywy serwisu. Upoważniony serwisant łączy się zdalnie z serwisowanym komputerem z wykorzystaniem oprogramowania zapewniającego poprawność i bezpieczeństwo połączenia (np. imPcRemote, TeamViewer lub podobne oprogramowanie). Wymaga się, aby serwisant przed rozpoczęciem zdalnego serwisu uzyskał na to zgodę osoby uprawnionej.

## X. Zasady bezpiecznego użytkowania sprzętu IT, dysków, programów

1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT zobowiązany jest do jego zabezpieczenia przed zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, kserokopiarki, laptopy i smartfony.
2. Użytkownik jest zobowiązany zgłosić zagubienie, utratę lub zniszczenie powierzonego mu sprzętu IT.
3. Samowolne instalowanie, otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) do lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
4. Użytkownik jest zobowiązany do usuwania plików z nośników/dysków, do których mają dostęp inni użytkownicy, nieupoważnieni do dostępu do takich plików (np. podczas współużytkowania komputerów).
5. Uprawniony do niszczenia nośników jest informatyk lub inna osoba, której Administrator danych poleci utylizację. Nośniki powinny być utylizowane na zasadach określonych w Instrukcji zarządzania systemami informatycznymi w p. VI. Użytkownik

jest zobowiązany do przekazania zgłoszenia informatykowi nośników przeznaczonych do zniszczenia.

6. Użytkownicy komputerów przenośnych na których znajdują się dane osobowe lub z dostępem do danych osobowych przez Internet zobowiązani są do stosowania zasad bezpieczeństwa zawartych Instrukcji zarządzania RODO.

## XI. Zabezpieczenie dokumentacji papierowej z danymi osobowymi

1. Upoważnieni pracownicy są zobowiązani do stosowania tzw. „**Polityki czystego biurka**". Polega ona na zabezpieczaniu (zamykaniu dokumentów oraz nośników np. w szafach, biurkach, pomieszczeniach) przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas nieobecności pracownika w pomieszczeniu, w trakcie godzin pracy.
2. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach lub utylizacji ich w specjalnych bezpiecznych pojemnikach z przeznaczeniem do bezpiecznej utylizacji.
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w innych pomieszczeniach.
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub pozostawiania ich na zewnątrz, w miejscach publicznych.
5. Podczas wykonywania pracy w terenie, jeżeli pracownicy przenoszą dokumenty powinni to robić w torbach z zabezpieczeniem ich przed otwarciem i dostępem do dokumentów osób nieupoważnionych. Po zamknięciu, torbę należy zabezpieczyć przed otwarciem przez osoby nieupoważnione. Zabrania się ujawniania sposobu otwarcia torby osobom nieupoważnionym.

## XII. Zasady wynoszenia nośników z danymi poza Spółkę

1. Użytkownicy nie mogą wynosić na zewnątrz wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Administratora. Do takich nośników zalicza się: wymienne twarde dyski, pen-drive, płyty CD, DVD, pamięci typu Flash.

2. Nośniki zawierające dane osobowe, które mogą zostać wyniesione poza teren PTBSu muszą być zaszyfrowane.
3. Należy zapewnić bezpieczne przewożenie nośników tak aby były chronione przed zagubieniem lub kradzieżą.
4. Do zapisywania plików z dokumentami zawierającymi dane osobowe nie mogą zostać wykorzystywane nośniki, które nie zostały zaakceptowane przez Administratora i zaszyfrowane.

## XIII. Zasady korzystania z Internetu

1. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów oraz zapisywania plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej (firma zewnętrzna świadcząca usługi informatyczne) lub Administratora i tylko w uzasadnionych przypadkach.
2. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane samowolnie.
3. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
4. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
5. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą ”https:”. Dla pewności należy „kliknąć” na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
6. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.
7. Zabrania się samowolnego podłączania do komputerów modemów, telefonów komórkowych i innych urządzeń dostępowych (np.: typu BlueConnect, iPlus, OrangeGo).

Zabronione jest też łączenie się przy pomocy takich urządzeń z Internetem w chwili, gdy komputer użytkownika podłączony jest do sieci wewnętrznej.

## XIV. Zasady korzystania z poczty elektronicznej

1. Przesyłanie danych osobowych z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione.
2. W przypadku przesyłania danych osobowych poza organizację należy wysyłać pliki zaszyfrowane/spakowane (np. programem 7 zip, winzipem, winrarem) i zahasłowane, gdzie hasło powinno być przesłane do odbiorcy inną metodą np. telefonicznie lub SMSem.
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6. **WAŻNE:** Nie otwierać załączników (.zip, .xlsm, .pdf, .exe) w mailach!!!!! Są to zwykle „wirusy", które infekują komputer oraz często pozostałe komputery w sieci. **WYSOKIE RYZYKO BEZPOWROTNEJ UTRATY DANYCH.**
7. **WAŻNE:** Nie wolno „klikać" na hiperlinki w mailach, gdyż mogą prowadzić do stron z „wirusami". Użytkownik „klikając" na taki link infekuje komputer oraz inne komputery w sieci. **WYSOKIE RYZYKO BEZPOWROTNEJ UTRATY DANYCH.**
8. Należy zgłaszać firmie zewnętrznej świadczącej usługi informatyczne przypadki podejrzanych emaili.
9. Użytkownikom nie wolno rozsyłać „niezawodowych" emaili w formie „łańcuszków szczęścia", np. życzenia świąteczne adresowane do kilkuset osób.
10. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW" w celu zamaskowani adresów innych odbiorców. Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości"!
11. Konta pocztowe służbowe są odseparowane od poczty prywatnej.
12. Służbowe konto pocztowe email jest przeznaczone do wykonywania obowiązków służbowych.

13. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
14. Zabrania się użytkownikom poczty elektronicznej konfigurowania swoich kont pocztowych do automatycznego przekierowywania wiadomości na adres zewnętrzny.
15. Korzystanie z maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.
16. Przy korzystaniu z maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego. Za nie przestrzeganie tych praw ponoszą osobistą odpowiedzialność.
17. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.

## XV. Ochrona antywirusowa

1. Użytkownicy zobowiązani są do skanowania programem antywirusowym plików wprowadzanych z zewnętrznych nośników, jeśli system antywirusowy taką funkcję posiada.
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów np. „Twój system jest zainfekowany!, zainstaluj program antywirusowy”, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie firmę zewnętrzną świadczącą usługi informatyczne lub Administratora.

## XVI. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych.

A. Nie zaleca się przechowywać zbędnych nośników informacji zawierających dane osobowe oraz kopii zapasowych, a także wydruków i innych dokumentów zawierających dane osobowe.
B. Po okresie przechowywania lub użyteczności, dane osobowe powinny zostać zniszczone tak, aby nie było możliwe ich odczytanie.

C. Dane osobowe zapisane na nośnikach elektronicznych, kopie zapasowe oraz wydruki i inne dokumenty zawierające dane osobowe przechowywane są w szafie pancernej lub w szafach zamykanych na klucz.

D. W przypadku uszkodzenia lub zużycia nośnika informacji, który zawiera dane osobowe należy go fizycznie zniszczyć w taki sposób, aby nie było możliwe odczytanie danych osobowych. W Spółce jest podpisana umowa na utylizację sprzętu komputerowego. Z utylizacji sporządzany jest protokół zniszczenia.

## XVII. Procedura zbierania informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia.

**1.** W systemie informatycznym służącym do przetwarzania danych osobowych zapisywane są informacje o odbiorcach danych, w tym imię i nazwisko lub nazwa odbiorcy, data udostępnienia oraz zakres udostępnienia. W przypadku, gdy w systemie informatycznym służącym do przetwarzania danych osobowych nie jest możliwe odnotowywanie takich informacji, użytkownik odnotowuje je w rejestrze umów powierzenia, który stanowi **załącznik nr 15** polityki bezpieczeństwa. Ze względów organizacyjnych dopuszcza się prowadzenie rejestru przez poszczególne działy Administratora, które nadzorują realizację zawartych umów powierzenia.

A. Rejestr ten prowadzi się w formie elektronicznej oraz papierowej.

B. Rejestr dotyczy tylko użytkowników uprawnionych do udostępniania danych osobowych, w tym pracujących i obsługujących programy (czy dane) umożliwiające takie udostępnienie.

## XVIII. Zasady kontroli na podstawie Instrukcji Zarządzania Systemem Informatycznym

A. Administrator oraz Inspektor Ochrony Danych Osobowych ma prawo do kontroli stanu zabezpieczeń oraz przestrzegania zasad ochrony danych osobowych raz w roku.

B. Kontrola winna być zakończona protokołem z wykonani czynności sprawdzających.

## XIX. Procedura postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego.

A. Każdy użytkownik w przypadku stwierdzenia uchybienia lub wystąpienia zagrożenia bezpieczeństwa systemu informatycznego ma obowiązek niezwłocznie powiadomić o tym fakcie Administratora, firmę informatyczną i/lub Inspektora Ochrony Danych Osobowych.

B. Procedurę postępowania z naruszeniami reguluje **załącznik nr 14** do Polityki Bezpieczeństwa, która znajduje zastosowanie do przypadków naruszenia bezpieczeństwa systemu informatycznego**.**