Załącznik
do Uchwały Nr 3/04/2019
Zarządu SM „Skarbek” z dnia 17.05.2019 r.

INSTRUKCJA
ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM
DO PRZETWARZANIA DANYCH OSOBOWYCH
W SPÓŁDZIELNI MIESZKANIOWEJ „SKARBEK” W WAŁBRZYCHU

I . Postanowienia ogólne

1. Niniejsza instrukcja określa zasady właściwego zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, które Spółdzielnia przetwarza jako ADO lub Procesor.

2. Celem wdrożenia instrukcji jest zadośćuczynienie obowiązującym przepisom prawa w zakresie ochrony danych osobowych przetwarzanych przez Spółdzielnię , określonych w przepisach krajowych i RODO oraz określenia warunków technicznych i organizacyjnych, jakim powinny odpowiadać wchodzące w skład tych systemów urządzenia, odpowiednio do kategorii danych objętych ochroną i skali zagrożeń .

3. Niniejsza instrukcja ma na celu zapewnienie regularnego testowania systemów informatycznych oceniając skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo danych osobowych .

4. W Spółdzielni funkcję administratora systemu informatycznego (ASI) pełni informatyk posiadający do wykonywania tych czynności uprawnienia ADO .

5. Instrukcja ma zastosowanie do wszystkich systemów informatycznych stosowanych w Spółdzielni do przetwarzania danych osobowych .

II. Obowiązki Administratora Danych Osobowych w zakresie zarządzania systemami informatycznymi

1. Nad środkami organizacyjnymi i technicznymi zapewniającymi ochronę danych osobowych przetwarzanych w systemach informatycznych odpowiednią do kategorii danych oraz zagrożeń sprawuje ADO, w szczególności zapewniając:

a/ pseudominimalizację , integralność
b/ zdolność do szybkiego przywrócenia dostępności danych i dostępu do nich w czasie incydentu fizycznego lub technicznego .

2. Do obowiązków ADO w zakresie zarządzania systemem informatycznym w szczególności należy:

a/ nadzór nad wdrożonymi zabezpieczeniami systemów informatycznych
b/ monitorowanie poziomu bezpieczeństwa przetwarzanych danych osobowych i podejmowanie decyzji o zastosowaniu innych środków organizacyjnych czy też technicznych zapewniających ochronę danych .

c/ wprowadzenie mechanizmu monitorowania w celu identyfikacji i zapobiegania zagrożeniom , w tym pozwalające na wykrycie prób nieautoryzowanego dostępu do informacji lub przekroczenia przyznanych uprawnień w systemie .

d/ nadzór nad nadawaniem , modyfikowaniem i odbieraniem uprawnień użytkowników do przetwarzania danych osobowych w systemach informatycznych

e/ nadzór nad stosowaniem środków bezpieczeństwa danych osobowych w tym postanowień niniejszej Instrukcji przez Użytkowników systemów informatycznych .

f/ współpraca z Administratorem Systemów Informatycznych (ASI) poprzez wydawanie zaleceń lub zatwierdzenie czynności w celu zapewnienia sprawnego funkcjonowania systemów informatycznych w tym zabezpieczeń , napraw lub utylizacji sprzętu wchodzącego w skład systemów lub z nim powiązanego .

g/ inne obowiązki związane z ochroną danych osobowych przetwarzanych w Spółdzielni

III. OBOWIĄZKI UŻYTKOWNIKÓW SYSTEMU INFORMATYCZNEGO

1. Każdy użytkownik systemu informatycznego w zakresie przetwarzania danych osobowych zobowiązany jest do :
1/ przestrzegania zasad przetwarzania danych osobowych procedur operacyjnych i bezpieczeństwa opracowanych dla systemu .

2/udostępniania danych osobowych wyłącznie osobom upoważnionym lub uprawnionym do ich uzyskania

3/ uniemożliwienie dostępu lub podglądu danych osobowych w systemie osobom nieupoważnionym/ ustawienie monitorów komputerów uniemożliwiające dostęp do danych osobom nieupoważnionym, ochrona ekranów komputerów wygaszaczami zabezpieczonymi hasłem, blokowanie komputera przed każdorazowym opuszczeniem stanowiska pracy.

4/ informowanie ADO lub ASI o wszelkich naruszeniach ,podejrzeniach naruszenia i nieprawidłowościach w sposobie przetwarzania i ochrony danych osobowych.

5/ informowanie ADO o wszelkich awariach czy też nieprawidłowościach w funkcjonowaniu systemu informatycznego lub urządzeń z nim związanych .

2. Użytkownikom systemu informatycznego zabrania się :

a. korzystania ze stanowisk komputerowych podłączonych do sieci informatycznej poza godzinami i dniami urzędowania bez pisemnej zgody ADO lub osoby upoważnionej ,

b. udostępniania stanowisk roboczych osobom nieuprawnionym,

c. wykorzystywania sieci komputerowej w celach innych niż wyznaczone przez ADO ,

d. samowolnego instalowania i używania programów komputerowych ,

e. korzystania z nielicencjonowanego oprogramowania oraz wykonywania jakichkolwiek działań niezgodnych u ustawą o ochronie praw autorskich,

f. umożliwiania dostępu do zasobów wewnętrznej sieci informatycznej oraz sieci internetowej osobom nieuprawnionym ,

g. używania komputera bez zainstalowanego lub działającego oprogramowania antywirusowego ,

IV. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZ UŻYTKOWNIKÓW SYSTEMU .

1. Użytkownik systemu przed przystąpieniem do pracy obowiązany jest dokonać sprawdzenia urządzeń informatycznych oraz swojego stanowiska pracy, zwracając szczególną uwagę na ewentualne okoliczności wskazujące na naruszenie ochrony danych osobowych .

2. W przypadku stwierdzenia lub podejrzenia , iż miało miejsce naruszenie ochrony danych osobowych Użytkownik systemu zobowiązany jest postępować zgodnie z instrukcją postępowania w sytuacji naruszenia danych zawartą w Polityce bezpieczeństwa .

3. Kończąc pracę , Użytkownik obowiązany jest do wylogowania się z systemu informatycznego, wyłączenia komputera i zabezpieczenia stanowiska pracy , w szczególności wszelkiej dokumentacji , wydruków oraz wymiennych nośników informacji , na których znajdują się dane osobowe i umieszczenia ich wewnątrz szaf lub w zamykanym biurku .

4. W sytuacjach awaryjnych oraz gdy zaistnieją nieprawidłowości w funkcjonowaniu systemu informatycznego Użytkownik powinien niezwłocznie przekazać informację o tej sytuacji do Administratora systemu, który z kolei powiadamia niezwłocznie o tym fakcie ADO oraz I OD, jeśli uzna zaistniałą sytuację za naruszenie polityki bezpieczeństwa danych osobowych . Użytkownik obowiązany jest postępować zgodnie z instrukcjami .

V. ZADANIA ADMINISTRATORA SYSTEMÓW INFORMATYCZNYCH

1. W Spółdzielni zadania i obowiązki Administratora Systemu Informatycznego (ASI) pełni informatyk .

2. ASI / informatyk jest odpowiedzialny za przestrzeganie zasad bezpieczeństwa, przetwarzania danych osobowych w zakresie systemu informatycznego a także kontrola przepływu informacji systemem informatycznym a siecią publiczną .

3. Do zadań ASI / Informatyka należy:

1/ Implementacja odpowiednich mechanizmów bezpieczeństwa w administrowanej infrastrukturze informatycznej .

2/ Merytoryczny nadzór w zakresie zachowania bezpieczeństwa przy przetwarzaniu danych .

3/ Nadzorowanie i aktualizacja programów antywirusowych .

4/ Zakładanie skrzynek pocztowych , przekazywanie danych do innych podmiotów w celu nadania uprawnień do systemów .

5/ Kontrola sprzętu informatycznego w zakresie przestrzegania Polityki Bezpieczeństwa Danych Osobowych .

6/ Nadzór nad zmianą haseł dla użytkowników systemu .

7/ Zapewnienie pomocy użytkownikom przy korzystaniu z systemu informatycznego .

8/ Tworzenie kopii zapasowych danych przechowywanych w systemie informatycznym .

9/ Monitorowanie poziomu bezpieczeństwa w systemie informatycznym, a w szczególności bieżącego stanu aktualizacji systemów operacyjnych i serwerów oraz sygnatur programów antywirusowych .

10/ Monitorowanie działania systemu informatycznego i przekazywanie informacji o zagrożeniach ADO .

11/ Aktywny udział w procesie reagowania na incydenty w zakresie bezpieczeństwa oraz usuwania ich skutków .

12/ Zarządzanie określonymi rozwiązaniami technicznymi związanymi z ochroną systemu informatycznego .

13/ Kontrolowanie przestrzegania zasad bezpiecznego przetwarzania danych w

systemie informatycznym .

a/ Czasowe przeglądy i weryfikacja m.in. :

***** rozmieszczenia stacji roboczych w poszczególnych pomieszczeniach,

*****sprawności użytkowanego sprzętu,

***** legalności zainstalowanego oprogramowania ,

***** poprawności instalacji nakładek systemowych i aktualizacji sygnatur wirusów programu antywirusowego ,

***** przyznanych uprawnień do systemów informatycznych .

b/ Nadzorowanie napraw sprzętu informatycznego oraz sieci teleinformatycznych

c/ Prowadzenie dokumentacji wykonanych czynności(w sposób papierowy lub informatyczny) zawierający rodzaj wykonanej czynności (zmianę konfiguracji sprzętu, naprawy sprzętu, instalację oprogramowania, incydenty) umiejscowienie, podpis

d/ stosowanie postanowień zawartych w regulaminie serwerowni .

VI. NADAWANIE UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Użytkownicy systemów informatycznych do przetwarzania danych osobowych przed dopuszczeniem do obsługi tych systemów powinni zostać zapoznani z przepisami krajowymi, RODO oraz Politykę bezpieczeństwa danych osobowych obowiązującą w Spółdzielni a także przeszkoleń z obsługi oprogramowania służącego do przetwarzania danych osobowych .
Użytkownicy systemów składają w tym zakresie stosowne oświadczenie .

2. O nadaniu użytkownikom uprawnień do przetwarzania danych osobowych w systemach informatycznych i zakresie tych uprawnień decyduje Zarząd Spółdzielni .

3. Spółdzielnia prowadzi ewidencję osób , którym wydano uprawnienia do przetwarzania danych osobowych .

4. Administrator systemu nadaje dla nowego konta użytkownika hasło tymczasowe i przekazuje je Użytkownikowi . Użytkownik przy pierwszym logowaniu zobowiązany jest zmienić hasło , ustanawiając nowe hasło .

5. Zmiany dotyczące Użytkownika , takie jak rozwiązanie umowy o pracę lub utrata upoważnienia wymagają natychmiastowego wyrejestrowania Użytkownika z systemu oraz unieważnienia hasła .

6. Dostęp do systemu oraz programów służących do przetwarzania danych osobowych powinien być możliwy tylko po podaniu identyfikatora odrębnego dla każdego użytkownika .

VII. PROCEDURY TWORZENIA KOPII ZAPASOWYCH /BEZPIECZEŃSTWA / .

1. Osobą odpowiedzialną za tworzenie kopii zapasowych (bezpieczeństwa) jest Administrator Systemów informatycznych / Informatyk .

2. Kopie zapasowe zbiorów danych osobowych tworzone są codziennie , po zakończonym dniu pracy w sposób automatyczny .

3. Kopie zapasowe są tworzone na sieciowym dysku zewnętrznym i przechowywane są w osobnym pomieszczeniu (pokój nr 18) przez okres obejmujący 60 dni wstecz .

4. Dostęp do kopii zapasowych ma Administrator systemu .

5. W razie braku możliwości utworzenia kopii zapasowych w sposób automatyczny , kopie zapasowe mogą być tworzone ręcznie przez Administratora Systemu na zewnętrznym nośniku pamięci , przeznaczonym tylko do tego celu .
Utworzone w w/w sposób kopie powinny zostać opisane w sposób umożliwiający identyfikację zawartych w nich dane osobowe .

VIII. METODY UWIERZYTELNIENIA

1. Spółdzielnia stosuje metody oraz środki uwierzytelniania , a także procedury związane z ich zarządzaniem i użytkowaniem .

2. Uwierzytelnianie użytkownika w systemie informatycznym następuje po podaniu użytkownikowi systemu informatycznego indyfikatora / loginu i hasła / .

3. Wszystkie komputery posiadają konto domenowe identyfikatory . Użytkowników do systemów informatycznych , które wraz z nadanymi uprawnieniami umożliwiają użytkownikom wykonywanie czynności zgodnych z zakresem obowiązków .

4. Przydziału identyfikatora / loginu i pierwszego hasła / dokonuje ASI/ informatyk .

5. Hasło powinno składać się z co najmniej 8 znaków i zawierać małe i wielkie litery oraz cyfry i znaki specjalne . I ich zmiana powinna być dokonywana co 90 dni . Hasła są utrzymywane w tajemnicy a w przypadku jego utraty , ASI tworzy nowe hasło tymczasowe , które Użytkownik zmienia zgodnie z pkt.4 Rozdziału VI .

6. Spółdzielnia posiada Internetowy system obsługi kontrahenta obejmujący lokale w zarządzanych i administrowanych zasobach , którego użytkownikiem może być każda

osoba posiadająca tytuł prawny do lokalu , która złoży stosowny wniosek o utworzenie indywidualnego konta w tym systemie . .

7. Dostęp do systemu , o którym mowa w pkt. 6 kontrahent uzyskuje poprzez nadany login i tymczasowe hasło (zmienione przez kontrahenta) .

IX. KOMPUTERY , PROGRAMY KOMPUTEROWE ZAWIERAJĄCE DANE OSOBOWE,SIECI/ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO

1. Dla każdej osoby , której dane osobowe są przetwarzane w systemie informatycznym z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie – system informatyczny zapewnia odnotowanie :

a) daty pierwszego wprowadzenia danych do systemu

b) identyfikatora Użytkownika wprowadzającego dane osobowe do systemu , chyba że dostęp do systemu informatycznego i przetwarzania z nim danych posiada jedna osoba

c) źródła danych, w przypadku zbierania danych , nie od osoby , której one dotyczą

d) informacji o odbiorcach danych , którym dane osobowe zostały udostępnione , oraz dacie i zakresie tego udostępniania , chyba , że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych .

e) wniesienia przez osobę , której dane są przetwarzane , sprzeciwu w przypadkach przewidzianych w stosownych przepisach .

2. Odnotowywanie informacji , o których mowa w ust 1 pkt. 1I 2 niniejszej Instrukcji automatycznie po zatwierdzeniu przez Użytkownika operacji wprowadzenia danych .

3. Stacje robocze / komputery służą wyłącznie do wykonywania obowiązków służbowych i zabronione jest wykorzystywanie ich do innych celów również użytkowania ich przez inne osoby niż użytkownicy, którym zostały one udostępnione

4. Na każdej stacji roboczej / komputerze przetwarzającej dane osobowe zainstalowane jest oprogramowanie antywirusowe .

5. Systemy antywirusowe zainstalowane na stacjach roboczych są skonfigurowane w celu :

a/ zablokowania możliwości ingerencji Użytkownika w ustawienia oprogramowania antywirusowego

b/ możliwości automatycznego uaktualnienia wzorców wirusowych

c/ możliwości zbierania informacji o wynikach pracy oprogramowania .

6. W przypadkach wystąpienia infekcji Użytkownik powinien opisać incydent i niezwłocznie powiadomić o tym fakcie ADO lub ASI / Informatyka .

W przypadku braku możliwości automatycznego usunięcia wirusów przez system antywirusowy ASI , podejmuje działania zmierzające do usunięcia zagrożenia .

7. Użytkownikom zabrania się instalacji na stacjach roboczych zewnętrznych programów w szczególności pochodzących z Internetu bez uzyskania zgody ASI .

8. Użytkownikom stacji roboczych zabrania się:

a/ kopiowania oraz utrwalania zawartości systemu informatycznego /danych osobowych/ lub plików je zawierających / i przekazywania ich poza obszar przetwarzania danych osobowych wskazany w Polityce bezpieczeństwa

b/ korzystania z prywatnych skrzynek poczty elektronicznej

c/ korzystania z prywatnych usług internetowych zapewniających przechowywanie danych w chmurze oraz transfer plików pomiędzy urządzeniami

d/ otwierania lub pobierania zawartości poczty elektronicznej nieznanego pochodzenia . W razie otrzymania takiej wiadomości Użytkownik niezwłocznie powiadomi o tym ASI i stosuje się do jego zaleceń .

X. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMU INFORMATYCZNEGO .

1. Przeglądy , naprawy i konserwacje systemu informatycznego oraz nośników informacji , które będą przeprowadzane w miejscu użytkowania tego systemu , są dokonywane przez Administratora systemu, są dokonywane przez Administratora systemu , z wyjątkiem sytuacji, kiedy niezbędnej naprawy dokonuje firma zewnętrzna lub producent sprzętu .

2. Za prawidłowość przeprowadzenia przeglądów , zapewnienia jakości , konserwację i dokumentowanie zmian w systemach odpowiada Administrator systemu .Przegląd programów i narzędzi programowych dokonywany jest w sposób bieżący, a w przypadku stwierdzenia nieprawidłowości w działaniu elementów systemu ASI podejmuje niezwłocznie czynności zmierzające do przywrócenia ich prawidłowego działania .

3. Jeżeli do przywrócenia prawidłowego działania systemu niezbędna jest pomoc podmiotu zewnętrznego to wszelkie czynności na sprzęcie komputerowym są dokonywane w obszarze przetwarzania danych osobowych. Jeśli jest to niemożliwe sprzęt może być wydany do naprawy w serwisie po otrzymaniu umowy powierzenia danych .

4. Podmiot zewnętrzny , który przetwarza dane osobowe na zlecenie administratora powinien działać na podstawie wymaganej prawej pisemnej umowy .

5. W przypadku wykorzystywania zdalnego dostępu do komputerów SM „Skarbek” przez firmę serwisującą należy ograniczyć dostęp wyłącznie do koniecznych zasobów .Firma serwisująca zobowiązana jest , aby w umowie określić nazwę oprogramowania używanego do pomocy zdalnej oraz właściciela licencji . Fakt wykorzystania połączenia zdalnego musi być odnotowany- data , godzina , zakres usług .

6. Urządzenia , dyski lub inne elektroniczne nośniki informacji zawierające dane osobowe, przeznaczone do naprawy pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie . Jeżeli jest to możliwe przekazuje się do naprawy na podstawie umowy powierzenia danych .

7. W przypadku naprawy sprzętu informatycznego w obszarze baz danych np. naprawa bazy naprawa wykonywana jest w obecności ADO . W przypadku niemożliwości naprawy w siedzibie ADO baza może być przekazana do naprawy wyłącznie na podstawie UPD.

W SM"Skarbek" naprawę sprzętu informatycznego zawierającego dane osobowe realizuje się na podstawie umowy powierzenia danych

8. Przynajmniej raz do roku ASI weryfikuje system informatyczny, obejmując w szczególności :

a) sprawdzenie , jakie programy są zainstalowane na stacjach roboczych i czy są one bezpieczne dla przetwarzanych w systemie informatycznych danych osobowych ;

b) sprawdzenie możliwości lub konieczności aktualizacji oprogramowania i ewentualnie dokonanie takiej aktualizacji ;

c) usunięcie oprogramowania uznanego za zagrażające bezpieczeństwu systemu lub przetwarzanych w nim danych osobowych .

9. W przypadkach , w których urządzenia, dyski lub inne elektroniczne nośniki informacji zawierające dane osobowe nie nadają do dalszej eksploatacji , ADO lub Administrator systemu za zgodę ADO zleca ich utylizację . Jeśli jest to możliwe sprzęt pozbawia się zapisu danych osobowych bądź uszkadza się nośniki w sposób uniemożliwiający odczytanie tych danych

XI KOMPUTERY I URZĄDZENIA PRZENOŚNE

1. Osoba użytkująca komputer przenośny, tablet, smartfon lub telefon zawierający dane osobowe zachowujesz szczególną ostrożność podczas jego transportu, przechowywania I użytkowania poza obszarem przetwarzania danych osobowych, w tym dodatkowo zabezpiecza hasłem pliki lub foldery zawierające dane osobowe.

2. Laptopy opuszczające SM SKARBEK posiadają szyfrowane dyski.

3. Zabrania się zapisywania załączników na urządzeniach mobilnych nieposiadających szyfrowania.

4. Przy korzystaniu z poczty firmowej za pomocą przeglądarki www należy zachować szczególne środki ostrożności polegające na:

a/ nie zapisywaniu identyfikatora/loginu i hasła w przeglądarce internetowej,

b/ nie zapisywaniu załączników zawierających dane osobowe,

c/ wylogowaniu się po zakończeniu korzystania z usługi.

5. Do łączenia się urządzeń mobilnych będących poza terenem przetwarzania danych z bazą urzędu służą tunele VPN.

XII DYSKI I INNE NOŚNIKI DANYCH

1. Urządzenia, dyski lub inne elektroniczne nośniki informacji zawierające dane osobowe podlegają ewidencji wg załącznika „Wykaz zewnętrznych nośników informacji" - stanowiący załącznik nr 10 do Polityki Bezpieczeństwa.

2. Zabrania się korzystania z własnych nośników danych.

3. Nośniki przeznaczone do:

a/ likwidacji – pozbawia się wcześniej zapisu danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,

b/ przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu danych w sposób uniemożliwiający ich odzyskanie,

c/ naprawy – pozbawia się wcześniej zapisu danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem ASI/INFORMATYK. Jeśli jest to niemożliwe przekazuje się do naprawy na podstawie umowy powierzenia danych.

4. Usuwanie danych osobowych utrwalonych na nośnikach elektronicznych następuje poprzez powierzenie tych nośników w celu usunięcia zapisanych na nich danych wyspecjalizowanej w tej dziedzinie firmie informatycznej lub poprzez nadpisanie usuwanych informacji przez ASI/INFORMATYKA w taki sposób, by nie istniała możliwość ich ponownego odczytania.

5. W celu usunięcia danych zapisanych na elektronicznych nośnikach ASI/INFORMATYKA może dokonać ich fizycznego uszkodzenia w taki sposób, by nie istniała możliwość odtworzenia zapisanych na nich danych.

XIII NARUSZENIE ZASAD BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO - INCYDENTY

W SM SKARBEK stosuje się następującą procedurę w przypadku stwierdzenia naruszenia zasad bezpieczeństwa systemu informatycznego:

1. W przypadku stwierdzenia przez użytkownika naruszenia zabezpieczeń przez osoby nieuprawnione jest on zobowiązany niezwłocznie poinformować o tym fakcie ASI/INFORMATYKA.

2. ASI/INFORMATYKA jest zobowiązany niezwłocznie podjąć czynności zmierzające do ustalenia przyczyn naruszeń zasad bezpieczeństwa i zastosować środki uniemożliwiające ich naruszanie w przyszłości.

3. ASI/INFORMATYK odnotowuje incydent i powiadamia o tym ADO.

4. ADO przeprowadza postępowanie mające na celu wyjaśnienie przyczyn oraz skutków incydentu.

XIV PRZESYŁANIE DANYCH POZA OBSZAR PRZETWARZANIA

1. Urządzenia i nośniki zawierające dane osobowe, przekazywane poza obszar przetwarzania zabezpiecza się w sposób zapewniający poufność i integralność danych, w szczególności poprzez zastosowanie ochrony kryptograficznej.

2. W wypadku przesyłania danych osobowych poza sieć przystosowaną do transferu danych osobowych należy zastosować szczególne środki bezpieczeństwa, które obejmują:

a/ zatwierdzenie przez ADO zakresu danych osobowych przeznaczonych do wysłania,

b/ zastosowanie mechanizmów szyfrowania danych osobowych,

c/ zastosowanie mechanizmów podpisu elektronicznego zabezpieczającego transmisję danych osobowych oraz rejestrację transmisji wysyłania danych osobowych,

d/ umożliwienie wysyłania danych osobowych tylko z wykorzystaniem określonej aplikacji i tylko przez określonych użytkowników

3. Administrator systemu informatycznego tworzy konfigurację mechanizmów kryptograficznych w sposób:

a/ zapewniający wykorzystanie obowiązujących wymagań w zakresie kryptograficznej ochrony danych osobowych,

b/ umożliwiający w miarę technicznych możliwości automatyczne szyfrowanie danych osobowych wysyłanych poza obszar przetwarzania danych,

c/ w przypadku, gdy podmiot zewnętrzny, z którym wymieniane są dane osobowe korzysta z innych mechanizmów kryptograficznych niż stosowane w SM SKARBEK, ASI może dopuścić zastosowanie tych mechanizmów lub mechanizmów z nimi zgodnych pod warunkiem zapewnienia zbliżonej do obowiązującej ochrony przesyłanych danych osobowych.

4. W SM SKARBEK wykorzystuje się wyłącznie służbowe skrzynki e-mail.

5. Skrzynki konfiguruje się w układzie pierwsza litera imienia i nazwisko@domena firmowa. Dopuszcza się adresy mailowe : *biuro@.....*

6. W przypadku korzystania z poczty elektronicznej nadawca zwraca uwagę na prawidłowość adresu odbiorcy oraz zabrania się wysyłania poczty zbiorczej. W

przypadku konieczności wysłania takich wiadomości korzystamy z UDW (Ukryty Dostawca Wiadomości).

7. Przy odbieraniu poczty z załącznikiem lub linkiem sprawdzamy czy nadawca jest znany, skanujemy wiadomość programem antywirusowym:

a/ zabrania się otwierania poczty niewiadomego pochodzenia,

b/ wykorzystuje się przy wysyłaniu pocztą danych osobowych certyfikat ID celem zaszyfrowania i zapewnienia integralności danych.

8. W przypadku wysyłania danych w formie tradycyjnej należy korzystać z firm kurierskich gwarantujących przewóz przesyłek poufnych lub przekazać pliki za pośrednictwem upoważnionej osoby:

- do transportu stosować bezpieczne koperty,
- poinformować odbiorcę o nadaniu przesyłki,
- odebrać informację o odbiorze przesyłki przez adresata, ewentualnie przesłać dane za potwierdzeniem odbioru.

XV MONITORING WIZYJNY

Zasady funkcjonowania monitoringów wizyjnych w zasobach zarządzanych i administrowanych przez Spółdzielnię określają odrębne regulaminy monitoringu zatwierdzane dla poszczególnych nieruchomości w których instalowane są monitoringi .

XVI POSTANOWIENIA KOŃCOWE

1. Użytkownicy systemu elektronicznego tresć niniejszej instrukcji otrzymają w wersji elektronicznej.Wersja papierowa znajdować się będzie w dziale członkowstwo-mieszkaniowym .

2. Niniejsza instrukcja wchodzi w życie z chwilą podjęcia uchwały Zarządu o jej wprowadzeniu tj, z dniem 17.05.2019 r.

Zarząd SM „Skarbek”