INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

w

PILSKIEJ SPÓŁDZIELNI MIESZKANIOWEJ LOKATORSKO-WŁASNOŚCIOWEJ W PILE

Dokumenty powiązane:

Polityka bezpieczeństwa w zakresie przetwarzania danych osobowych

Spis treści

§1

Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Pilskiej Spółdzielni Mieszkaniowej Lokatorsko-Własnościowej w Pile (zwaną dalej Instrukcją) została utworzona w związku z wymaganiami zawartymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2014 r. poz. 1182) oraz rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych Dz. U. z 2004 r. Nr 100, poz. 1024. Opracowany dokument jest zgodny z dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osób oraz ochrony prywatności w sektorze komunikacji elektronicznej.

§2

Instrukcja jest wewnętrznym dokumentem w Pilskiej Spółdzielni Mieszkaniowej Lokatorsko-Własnościowej w Pile i ma zastosowanie do wszelkich danych osobowych znajdujących się, bądź mogących znajdować się w systemie informatycznym Spółdzielni.

§3

Instrukcja określa:

1. sposób przydziału haseł dla użytkowników i częstotliwości ich zmiany oraz wskazuje osobę odpowiedzialną za te czynności,
2. sposób rejestrowania i wyrejestrowywania użytkowników oraz wskazuje osobę odpowiedzialną za te czynności,
3. procedury rozpoczęcia i zakończenia pracy,
4. metodę i częstotliwości tworzenia kopii awaryjnych,
5. metodę i częstotliwości sprawdzania obecności wirusów komputerowych oraz metodę ich usuwania,
6. sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków,
7. sposób dokonywania przeglądów i konserwacji systemu i zbiorów danych osobowych,
8. zasady korzystania z komputerów przenośnych,
9. sposób postępowania w zakresie komunikacji w sieci komputerowej.

§4

Instrukcja ma na celu zapewnienie procedur i właściwych warunków zarządzania systemem informatycznym dla ochrony zgromadzonych tam danych, jak również jednolitych i bezpiecznych zasad korzystania z tych danych przetwarzanych w systemie informatycznym oraz w dokumentacji Spółdzielni.

§ 5

Realizację zamierzeń określonych w § 4 gwarantuje następująca strategia:

1. przeszkolenie użytkowników w zakresie ochrony danych osobowych oraz zaznajomienie z przepisami dotyczącymi tych ochrony danych,
2. korzystanie z oprogramowania systemowego i użytkowego spełniającego wysokie standardy,
3. wykorzystywanie w systemie informatycznym zabezpieczeń gwarantujących nienaruszoną pracę systemu, w tym najnowszych wersji oprogramowania antywirusowego,
4. przypisanie użytkownikom określonych identyfikatorów i haseł, co pozwoli na jednoznaczną identyfikację użytkownika w środowisku systemowym,
5. ocena ewentualnych zagrożeń bezpieczeństwa systemu informatycznego i ryzyka związanego z jego obsługą ,
6. wdrożenie zabezpieczeń o charakterze fizycznym pomieszczeń , stosownie do zagrożeń i ryzyka wynikającego z oceny, o której mowa w pkt.5,
7. stałe monitorowanie wdrożonych zabezpieczeń w celu identyfikacji podatnych na zagrożenia obszarów i słabości zabezpieczeń,
8. okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych oraz podejmowanie niezbędnych działań dla likwidacji słabych ogniw w systemie zabezpieczeń.

Definicje

§ 5

Następujące pojęcia użyte w niniejszym dokumencie oznaczają:

dane osobowe - to każda informacja dotycząca osoby fizycznej, pozwalająca na identyfikacje tożsamości tej osoby,

przetwarzanie danych - to wszelkie operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

administrator danych – Administrator Danych Osobowych - *zarząd PSM L-W w Pile,*

administrator bezpieczeństwa informacji - ABI - wyznaczona osoba odpowiedzialna za nadzorowanie przestrzegania zasad ochrony danych osobowych przetwarzanych w systemach informatycznych oraz w dokumentacji *PSM L-W w Pile,*

administrator systemu informatycznego - ASI - informatyk odpowiedzialny za sprawne funkcjonowanie sieci komputerowej i oprogramowania zainstalowanego na serwerach i stacjach roboczych,

osoba upoważniona - użytkownik - osoba posiadająca upoważnienie wydane przez administratora danych i dopuszczona w zakresie w nim wskazanym jako użytkownik do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład,

użytkownik danych – każdy pracownik Spółdzielni, który wykonując czynności służbowe, przetwarza dane osobowe, tzn. wykonuje na nich operacje takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, czy usuwanie,

osoba uprawniona – osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych do wykonywania w jego imieniu określonych czynności,

osoba trzecia - to każda osoba nieupoważniona i przez to nieuprawniona do dostępu do danych osobowych lub zbiorów tych danych. Osobą trzecią jest również osoba posiadająca upoważnienie wydane przez administratora w zakresie czynności przekraczających ramy udzielonego jej upoważnienia,

sieć telekomunikacyjna – sieć o definicji zawartej w Ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2004r. Nr 171, poz. 1800, z późniejszymi zmianami),

sieć lokalna – połączenie funkcjonujących w Spółdzielni systemów informatycznych i stacji roboczych przy wykorzystaniu urządzeń i sieci telekomunikacyjnych,

stacja robocza – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom dostęp do danych znajdujących się w tym systemie,

system informatyczny – zespół współpracujących ze sobą urządzeń, programów, połączeń sieciowych i narzędzi programowych zastosowanych w celu przetwarzania danych,

bezpieczeństwo systemu informatycznego – wdrożone przez ABI lub osobę przez niego uprawnioną, środki organizacyjne i techniczne w celu zabezpieczenia oraz ochrony danych przed nieautoryzowanym dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem,

system przetwarzania danych – ta część systemu informatycznego oraz te procedury przetwarzania dokumentów papierowych, które razem tworzą system współpracujących ze sobą mechanizmów wykorzystywanych przy przetwarzaniu danych w Spółdzielni,

integralność danych – właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

poufność danych – właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom i osobom,

zbiór danych osobowych – każdy posiadający strukturę logiczną zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Sposób przydziału haseł i identyfikatorów dla użytkowników i częstotliwość ich zmiany

§7

1. Mając na względzie, iż systemy informatyczne przetwarzające dane osobowe są wyposażone w mechanizmy uwierzytelnienia użytkownika oraz kontroli dostępu do tych danych - dla każdej osoby upoważnionej ustalany jest odrębny identyfikator i hasło.

2. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.

3. Hasła dostępu i identyfikatory przyznawane są indywidualnie dla każdego z użytkowników i znane są tylko właścicielowi .

§8

Identyfikator użytkownika:

1. jest niepowtarzalny,
2. po wyrejestrowaniu użytkownika z systemu informatycznego nie jest przydzielany innej osobie,
3. użytkownicy zobowiązani są do zachowania w tajemnicy ustalonych dla nich identyfikatorów/haseł,
4. jest wpisywany do ewidencji osób zatrudnionych przy przetwarzaniu danych wraz z imieniem i nazwiskiem użytkownika,
5. za ochronę identyfikatora odpowiada użytkownik.

§9

Hasło użytkownika:

1. jest przydzielane indywidualnie dla każdego z użytkowników i znane tylko użytkownikowi, który się nim posługuje,
2. zostaje zmienione przy pierwszym zastosowaniu (zalogowaniu użytkownika) po przydzieleniu przez ASI,
3. nie jest zapisywane w systemie w postaci jawnej,
4. jest zmieniane raz na miesiąc,
5. jest utrzymywane w tajemnicy, również po upływie jego ważności.

§10

1. Osobą odpowiedzialną w Spółdzielni za sposób przydziału haseł dla użytkowników i częstotliwości ich zmiany jest ASI.
2. Rejestr identyfikatorów prowadzi ASI.
3. Hasła systemowe do urządzeń dostępowych, serwerów, urządzeń infrastruktury informatycznej itp. Przechowywane są w zapieczętowanej kopercie, w miejscu wyznaczonym przez ASI.

§11

Przydziału i zmiany haseł dokonuje się w następujący sposób:

1. wymogiem niezbędnym jest przydział haseł alfanumerycznych skonstruowanych co najmniej z 8 (ośmiu) znaków,
2. hasła są zmieniane przez każdego z użytkowników co najmniej raz na miesiąc,
3. zachowując wymóg zmieniania haseł co najmniej raz na miesiąc, użytkownik dba o to by hasła nie powtarzały się,
4. hasła nie mogą składać się z kombinacji znaków mogących prowadzić do odszyfrowania ich przez osoby trzecie (nieupoważnione),
5. niezależnie od wymogu zmieniania haseł każdego z użytkowników co najmniej raz na miesiąc, hasło winno być zmienione niezwłocznie w przypadku powzięcia podejrzenia lub stwierdzenia, że z hasłem mogły zapoznać się osoby trzecie.

§12

1. Użytkownik odpowiedzialny jest za wszystkie czynności wykonywane przy użyciu hasła, którym się posługuje lub posługiwał.
2. Użytkownik obowiązany jest utrzymywać hasła, którymi się posługuje lub posługiwał, w ścisłej tajemnicy, co obejmuje w szczególności dołożenie przez niego wszelkich starań w celu uniemożliwienia zapoznania się z nim przez osoby trzecie nawet po ustaniu jego ważności.
3. W przypadku powzięcia przez użytkownika podejrzenia lub stwierdzenia, że z hasłem mogły zapoznać się osoby trzecie, obowiązany jest on niezwłocznie zmienić hasło i powiadomić o tym ABI.
4. Użytkownicy obowiązani są utrzymywać hasła w tajemnicy również po upływie ich ważności.

Sposób rejestrowania i wyrejestrowywania użytkowników

§ 13

1 Rejestracji i wyrejestrowania użytkowników dokonuje ASI, który w imieniu Administratora prowadzi ich ewidencją, w oparciu o gromadzone wnioski o przyznanie i /lub modyfikację uprawnień, *(wzór formularza - załącznik nr 1.*

2. Jakakolwiek zmiana w zakresie informacji zawartych w ewidencji podlega natychmiastowemu odnotowaniu.

§14

1. Każda osoba jest rejestrowana w systemie informatycznym, jako użytkownik po spełnieniu następujących warunków:
   a) złożeniu wniosku przez przełożonego osoby ubiegającej się do ADO o udzielenie tej osobie dostępu do przetwarzania danych osobowych *(załącznik nr 1 do Instrukcji),*
   b) podpisaniu przez osobę ubiegającą się o dostęp oświadczenia o zapoznaniu się z przepisami o ochronie danych osobowych i obowiązku zachowania w tajemnicy informacji dotyczących ich przetwarzania (*załącznik nr 3 do Polityki Bezpieczeństwa*),
   c) wydaniu przez ADO lub osobę upoważnioną, upoważnienia do przetwarzania danych (*załącznik nr 2 do Polityki Bezpieczeństwa*).

§15

Upoważnienie oraz oświadczenie, o których mowa w § 14 pracownik prowadzący sprawy kadrowe dołącza do akt osobowych pracownika.

§ 16

1. Z chwilą zarejestrowania w systemie informatycznym, zgodnie z postanowieniami § 14, dana osoba jest informowana przez ASI o ustalonym dla niej identyfikatorze i konieczności posługiwania się hasłami.

2. Bez spełnienia wymogów wynikających z § 14 , ASI nie może zarejestrować jakiejkolwiek osoby w systemie informatycznym.

§17

1. Użytkownik jest wyrejestrowywany z systemu informatycznego na wniosek przełożonego. W każdym przypadku utraty przez niego uprawnień do dostępu do danych osobowych, co ma miejsce w przypadku:
   - ustania zatrudnienia tego użytkownika w Spółdzielni, bądź
   - zmiany zakresu obowiązków tego użytkownika,

o czym informację ASI uzyskuje od pracownika prowadzącego sprawy kadrowe lub bezpośredniego przełożonego użytkownika.

§18

W przypadkach wskazanych w § 17 co do użytkownika, który utracił uprawnienia do dostępu do systemu informatycznego, ASI dokonuje niezwłocznie następujących czynności:
1. blokuje jego profil, co powoduje, że osoba ta nie ma możliwości „zalogowania się" do sieci lub aplikacji,
2. dezaktywuje jego identyfikator,
3. podejmuje inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych w Spółdzielni.

§19

1. Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi.
2. ASI obowiązany jest gromadzić odrębnie identyfikatory, które utraciły ważność.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy

§20

1. Przed przystąpieniem do pracy w systemie użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych służących do przetwarzania danych osobowych oraz dokonać oględzin swojego stanowiska pracy, ze szczególnym uwzględnieniem czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.
2. Każdy użytkownik rozpoczynając pracę obowiązany jest „zalogować się" do systemu komputerowego posługując się swoim identyfikatorem i hasłem, dokładając jednocześnie szczególnej staranności w tym, aby przy tych czynnościach osoby trzecie nie powzięły wiadomości o treści używanego przez niego hasła. Następnie po podaniu dodatkowego hasła użytkownik ma możliwość „zalogowania się" do aplikacji zawierających dane osobowe.
3. Bez wykonania procedury opisanej w pkt. 1 i 2 jakakolwiek praca w systemie komputerowym nie jest możliwa.

§22

1. Maksymalna ilość prób wprowadzenia hasła przy logowaniu się do systemu wynosi 3 (trzy).
2. Po przekroczeniu liczby prób logowania system blokuje dostęp do zbioru danych na poziomie danego użytkownika.
3. Użytkownik informuje ASI lub swego bezpośredniego przełożonego o zablokowaniu dostępu do zbioru danych.
4. ASI ustala przyczyny zablokowania systemu oraz w zależności od zaistniałej sytuacji, podejmuje odpowiednie działania.

§23

1. W przypadku bezczynności użytkownika na komputerze stacjonarnym przez okres dłuższy niż 15 minut automatycznie włączany jest wygaszacz ekranu.
2. Wygaszacze ekranu powinny być zaopatrzone w hasła. Regulacje odnoszące się do haseł używanych przez użytkownika przy logowaniu, stosuje się odpowiednio do haseł wygaszacza.
3. Przed opuszczeniem miejsca pracy, użytkownik obowiązany jest poczekać aż zaktywizuje się wygaszacz, samemu zaktywizować wygaszacz lub w inny sposób zablokować stacje roboczą.
4. W przypadku, gdy przerwa w pracy trwa dłuższy okres oraz kończąc pracę użytkownik obowiązany jest „wylogować się" z aplikacji i systemu komputerowego oraz sprawdzić czy nie zostały pozostawione bez zamknięcia nośniki informacji. Opuszczając stanowisko użytkownik zamyka używane przez niego szafy i pomieszczenia, w których przechowuje się dokumentację i nośniki informacji.

§24

W przypadku zauważenia przez użytkownika naruszenia zabezpieczenia systemu informatycznego, zauważenia, że stan urządzenia, wartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń danych osobowych, obowiązany on jest niezwłocznie poinformować o tym fakcie swojego przełożonego i ABI.

Zasady korzystania z komputerów przenośnych, na których są przetwarzane dane osobowe poza siedzibą Spółdzielni

§25

Przetwarzanie danych osobowych na komputerach przenośnych poza siedzibą Spółdzielni, powinno być ograniczone do niezbędnego minimum i może się odbywać wyłącznie na podstawie pisemnej zgody ADO. Zakres, czas oraz miejsce przetwarzania powinno być ustalone przez przełożonego pracownika i uzgodnione z ABI oraz ASI.

§26

1. Pracownik korzystający z komputera przenośnego do przetwarzania danych osobowych lub dokumentów stanowiących tajemnicę służbową, zwłaszcza mających charakter lokalnej bazy lub pliku czyli zlokalizowanych bezpośrednio na użytkowanym komputerze i przetwarzanie których odbywa się poza obszarem przetwarzania danych określonych w „Polityce bezpieczeństwa Pilskiej Spółdzielni Mieszkaniowej Lokatorsko-Własnościowej w Pile", zobowiązany jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed zniszczeniem. W związku z powyższym użytkownik komputera przenośnego zobowiązany jest do:
   a. transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia,
      a w szczególności:
      I. transportowania komputera w odpowiedniej, przeznaczonej do tego celu torbie jako bagażu poręcznego,
      II. nie pozostawiania komputera w samochodzie, przechowalni bagażu, środkach transportu publicznego itp,
   b. korzystania z komputera w sposób minimalizujący ryzyko podejrzenia przetwarzanych danych przez osoby nieupoważnione, w szczególności zabrania się korzystania z komputera w miejscach publicznych i w środkach transportu publicznego,
   c. zdecydowanego uniemożliwienia korzystania z komputera osobom niepowołanym (np. rodzinie, dzieciom, znajomym),

d. zabezpieczenia komputera przenośnego hasłem i utrzymanie konfiguracji oprogramowania systemowego w stanie wymuszającym korzystanie z tego hasła,

e. wykorzystywanie haseł odpowiedniej jakości zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe,

f. zmianę haseł zgodnie z harmonogramem przyjętym w Spółdzielni,

g. blokowania dostępu do komputera przenośnego w przypadku, gdy nie jest on wykorzystywany przez pracownika,

h. regularnego i częstego kopiowania danych przetwarzanych na komputerze przenośnym, do systemu informatycznego Spółdzielni w celu umożliwienia wykonania kopii awaryjnej,

i. cyklicznego podłączania komputera do sieci informatycznej Spółdzielni w celu wykonania aktualizacji wzorców wirusów w programie antywirusowym,

§27

ASI zobowiązany jest do podjęcia działań mających na celu zabezpieczenie komputerów przenośnych, w szczególności:

1) dokonać konfiguracji oprogramowania w sposób wymuszający korzystanie z haseł odpowiedniej jakości oraz ich cyklicznej zmiany, zgodnie z wytycznymi dotyczącymi polityki posługiwania się hasłami w systemie informatycznym Spółdzielni,

2) w przypadku przetwarzania danych osobowych znajdujących się bezpośrednio na komputerze przenośnym - zabezpieczyć je dodatkowo poprzez wykorzystanie oprogramowania szyfrującego

3) dokonywać instalacji i konfiguracji oprogramowania antywirusowego,

4) przeprowadzić aktualizację wzorców wirusów zgodnie z zasadami zarządzania programem antywirusowym.

§ 28

ASI jest odpowiedzialny za prowadzenie ewidencji komputerów przenośnych wykorzystywanych do przetwarzania danych poza siedzibą Spółdzielni. W szczególności ewidencja powinna obejmować:

a. typ i numer seryjny komputera przenośnego,
b. imię i nazwisko osoby będącej użytkownikiem komputera,
c. wykaz oprogramowania zainstalowanego na komputerze, służącego do przetwarzania danych osobowych
d. rodzaj i zakres danych osobowych przetwarzanych na komputerze.

§ 29

W razie zgubienia lub kradzieży komputera przenośnego, pracownik zobowiązany jest do natychmiastowego powiadomienia ABI lub osoby uprawnionej zgodnie z zasadami informowania w przypadku naruszenia ochrony danych osobowych.

Metoda i częstotliwość tworzenia kopii awaryjnych oraz likwidacja nośnika informacji

§30

Tworzenie, przechowywanie i likwidację kopii bezpieczeństwa regulują szczegółowe instrukcje operacyjne dla poszczególnych aplikacji i systemów przetwarzania oraz specyficzne akty prawne (w zależności od rodzaju organizacji np. Ustawa o rachunkowości, Bankowa i inne) i niniejsza instrukcja.

§31

Wydruki komputerowe z systemu zawierające dane osobowe są:

- sporządzane jedynie dla celów operacyjnych,
- odpowiednio opisane i oznakowane,
- elementem archiwum papierowego i podlegają zasadom dotyczącym przetwarzania danych osobowych

w systemie tego archiwum,
- przechowywane są w odpowiednich zamykanych szafach i używane do celów operacyjnych przez określony czas wykorzystywania.

§31

1. Kopie bezpieczeństwa systemów i danych przechowywanych na serwerach sieciowych tworzone są automatycznie po każdym dniu roboczym i składowane na wydzielonych nośnikach informacji.
2. Administrator sieci nie rzadziej niż raz w miesiącu sprawdza możliwość odczytu z wykonanych kopii.
3. Kopie bezpieczeństwa, o których wyżej mowa, dla komputerów nie pracujących w sieci, tworzą użytkownicy na zewnętrznych nośnikach pamięci nie rzadziej niż raz w miesiącu.
4. Wszyscy pracownicy zobowiązani są przestrzegać terminów sporządzania kopii zapasowych oraz okresowo dokonywać kontroli możliwości odczytu danych zapisanych na tych kopiach.
5. Kopie bezpieczeństwa tworzone są:
   a) w celu zabezpieczenia danych na wypadek awarii urządzeń, na których są one przetwarzane,
   b) na odpowiednio opisanych oznakowanych nośnikach magnetycznych,
   c) przechowywane jak materiały zastrzeżone w wyznaczonym przez ABI pomieszczeniu,
   d) kopie bezpieczeństwa są przechowywane w szafie zamykanej na klucz , do której mogą mieć dostęp wyłącznie osoby upoważnione przez Administratora.

§32

1. Kopiowanie danych osobowych na nośniki informacji i robienie wydruków tych danych jest zabronione, chyba że konieczność ich sporządzenia wynika z nałożonego na użytkownika zakresu obowiązków i jest uzasadniona potrzebą ich wykonania oraz dozwolona przepisami prawa.
2. Wykorzystywanie nośników informacji lub wydruków w innym celu niż wskazany w ust.1 jest zakazane.

§33

1. Kopie bezpieczeństwa po ustaniu ich użyteczności są bezzwłocznie usuwane.
2. Kopie bezpieczeństwa, które uległy uszkodzeniu podlegają natychmiastowemu zniszczeniu.
3. Niszczenia kopii zapasowych na nośnikach magnetycznych dokonuje ASI lub upoważniona przez niego osoba.
4. Z nośników magnetycznych dane należy usunąć w sposób uniemożliwiający ich odczytanie, a w przypadku, gdy usunięcie danych nie jest możliwe, nośniki podlegają zniszczeniu w stopniu uniemożliwiającym dostęp do zawartych na nich danych.
5. Z nośników podlegających zniszczeniu nie wolno sporządzać wydruków.
6. Jeżeli dysk twardy jest uszkodzony i nie ma możliwości skasowania z niego danych osobowych należy wymontować go z komputera i fizycznie zniszczyć.
7. Likwidacji wydruków dokonuje się przy użyciu przeznaczonych do tego celu urządzeń (np. niszczarek).
8. Urządzenia, dyski lub inne informatyczne nośniki informacji, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie, czego dokonać można w szczególności poprzez zniszczenie ich w sposób trwały, tj. przez ich mechaniczne zniszczenie.
9. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe. przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych, pozbawia się zapisu tych danych.
10. Trwałego zniszczenia zbędnych nośników informacji i wydruków komputerowych dokonuje się na bieżąco w czasie pracy, nie później jednak niż przed opuszczeniem stanowiska pracy.

Metoda i częstotliwość sprawdzania obecności wirusów komputerowych oraz metoda ich usuwania.

§34

1. Serwery sieciowe i stacje lokalne wyposażone są w programy antywirusowe, które automatycznie na bieżąco monitorują pracę tych komputerów, wykrywają zagrożenia i je usuwają.
2. Programy antywirusowe aktualizowane są automatycznie w miarę pojawiania się aktualizacji za pomocą programowego scentralizowanego systemu dystrybucji aktualizacji.
3. W komputerach nie włączonych w sieć aktualizacji programów antywirusowych dokonuje administrator sieci w miarę potrzeb, nie rzadziej niż raz w miesiącu.

§35

Kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.

§36

1. O każdorazowym wykryciu wirusa przez oprogramowanie monitorujące użytkownik obowiązany jest niezwłocznie poinformować swojego przełożonego.
2. W razie niemożności usunięcia wirusa, administrator sieci ma obowiązek niezwłocznego przedstawienia Administratorowi lub wyznaczonej przez niego osobie, propozycji działań zaradczych.
3. W sytuacji korzystania z usług specjalistów zewnętrznych należy podjąć działania uniemożliwiające tym osobom dostęp do danych osobowych

§37

1. Po usunięciu wirusa administrator sieci sprawdza system informatyczny oraz przywraca go do pełnej funkcjonalności i sprawności.
2. Administrator sieci - jeżeli zachodzi taka konieczność - wnioskuje do Administratora o zakup nowego programu antywirusowego.
3. Administrator sieci prowadzi rejestr przypadków zainfekowania komputerów i nośników wykorzystywanych do przetwarzania danych osobowych w systemie.Sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych

§38

Przeglądów i konserwacji sprzętu komputerowego dokonuje się w miarę potrzeb wynikających z obciążenia sprzętu komputerowego, warunków zewnętrznych, w których eksploatowane są dane urządzenia oraz ważności sprzętu dla funkcjonowania całości systemu informatycznego.

§39

1. Prace dotyczące przeglądów, konserwacji i napraw wymagające autoryzowanych firm zewnętrznych, są wykonywane przy udziale ASI.
2. W wypadku konieczności dostępu do danych osobowych przez serwisantów, podpisują oni oświadczenie o zachowaniu tajemnicy (zgodnie z art.39 Ustawy o ochronie danych osobowych).
3. Urządzenia, dyski lub inne informatyczne nośniki informacji, przeznaczone do napraw, gdzie wymagane jest zaangażowanie autoryzowanych podmiotów zewnętrznych, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem ASI lub upoważnionej przez niego osoby.

Postanowienia końcowe

§ 40

Wszyscy pracownicy są zobowiązani do zapoznania się z treścią niniejszej polityki.

§ 41

Polityka bezpieczeństwa wchodzi w życie z dniem podpisania.

§ 42

Jakiekolwiek zmiany wprowadzane w załącznikach do niniejszego dokumentu nie wymagają zmiany zarządzenia, które wprowadziło niniejszą instrukcję w życie.

Spis załączników

Załącznik nr 1 „**Wniosek o nadanie uprawnień/zmianę uprawnień/odwołanie uprawnień*) w systemie ZSI”**

Załącznik nr 1

....dnia

..... r.
Imię i nazwisko wnioskującego

.....
Stanowisko wnioskującego

Wniosek
o nadanie uprawnień/zmianę uprawnień/odwołanie uprawnień*) w systemie ZSI UNISOFT

Dane użytkownika:

Imię i nazwisko:	
Stanowisko służbowe:	
Telefon:	

Wnioskuję o:
Założenie konta w systemie i nadanie uprawnień*)
Zmianę uprawnień na wymienione poniżej*)
Zablokowanie konta*)

Wnioskowane uprawnienia dotyczą systemu informatycznego :

	Nazwa modułu	**Opis uprawnień**	**Uwagi** (np. tylko odczyt/edycja)

Uprawnienia będą przyznane:*)

[ ] na okres od ..... r. do ..... r.*)

[ ] na czas nieokreślony*)

.....
Data i podpis wnioskującego

Administrator Systemu Informatycznego

Nadany identyfikator:

Uwagi:

.....
Data i podpis Administratora Systemu Informatycznego

* Niepotrzebne skreślić