ZRZĄDZENIE WEWNETRZNE NR 7/2010

Prezesa Zarządu Miejskiego Zakładu Gospodarki Komunalnej Sp. z o.o. w Nowej Soli
z dnia 30.08.2010

W sprawie : zatwierdzenia i przyjęcia do stosowania Instrukcji Zarządzania Systemem Informatycznym.

§1

W celu zabezpieczenia prawidłowego przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych przyjmuje się do stosowania Instrukcje Zarządzania Systemem Informatycznym, która stanowi Załącznik nr 1 do niniejszego zarządzenia wewnętrznego.

§2

Za wdrożenie Instrukcji odpowiada firma „Nova Komputery" w imieniu której działa p. Marek Śledzik, a za przestrzeganie jej postanowień kierownicy działów.

Do pełnienia funkcji Administratora Bezpieczeństwa Informacji został powołany Kierownik działu Administracyjno - Organizacyjnego – Pan Piotr Małek.

§3

Zobowiązuje się wszystkich pracowników korzystających z komputerów służbowych i będących użytkownikami systemu komputerowego do zapoznania się z postanowieniami w/w instrukcji i bezwzględnego jej stosowania.

§4

Zarządzenie wchodzi w życie z dniem 1.09.2010 r.

PREZES ZARZĄDU

Waldemar Wrześniak

INSTRUKCJA

Zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Miejski Zakład Gospodarki Komunalnej w Nowej Soli 2010

§1.

PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM ORAZ WSKAZANIE OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI

1. **A**dministratora **D**anych **O**sobowych (ADO) udziela Pracownikowi upoważnienia do przetwarzania danych osobowych na formularzu, którego wzór stanowi **załącznik nr 1** do niniejszego dokumentu.
2. Jeżeli przetwarzanie danych osobowych odbywa się w systemie informatycznym, Pracownik występuje do **A**dministratora **B**ezpieczeństwa **I**nformacji (ABI) o:
    a. założenie konta w Systemie Informatycznym MZGK, jeżeli pracownik jeszcze takiego konta nie posiada,
    b. przyznanie uprawnień w systemach informatycznych przetwarzających dane osobowe w MZGK na formularzu, którego wzór stanowi **załącznik nr 2** do niniejszego dokumentu.
3. ABI sprawdza przed wydaniem upoważnienia do przetwarzania danych osobowych czy użytkownik spełnia warunki dopuszczenia do przetwarzania danej grupy informacji, a w szczególności:
    a. czy użytkownik przeszedł szkolenie z zakresu bezpieczeństwa informacji Przedsiębiorstwa, w tym ochrony danych osobowych;
    b. czy stanowisko pracy użytkownika, w tym systemy informatyczne, spełnia warunki dopuszczenia do przetwarzania danych osobowych zgodnie z par. 5 Polityki Bezpieczeństwa;
    c. czy użytkownik podpisał oświadczenie o tajemnicy, według wzoru w **załączniku nr 3** do niniejszego dokumentu.
4. Jeżeli któryś z warunków nie jest spełniony Administrator Bezpieczeństwa Informacji w porozumieniu z zainteresowanym ustala sposób i termin uzupełnienia braków, o których mowa w pkt. 3 lit. a-c, lub odmawia przyznania identyfikatora/uprawnień.
5. Jeżeli użytkownik i jego stanowisko pracy spełniają warunki dopuszczenia, Administrator Bezpieczeństwa Informacji przekazuje wnioski do Administratora Systemu i Sieci (ASiS).
6. Administrator Systemu i Sieci tworzy identyfikator, zakłada konto oraz przyznaje lub zmienia uprawnienia w systemie komputerowym. Jeśli we wniosku określono czas obowiązywania uprawnienia ASiS ustawia taką ważność dla tego konta.
7. Na pisemny wniosek (**załącznik nr 4**) Administratora Bezpieczeństwa Informacji Administrator Systemu i Sieci blokuje lub usuwa konto w systemie komputerowym.
8. Na pisemny wniosek (**załącznik nr 5**) Administratora Bezpieczeństwa Informacji Administrator Systemu i Sieci zmienia lub usuwa uprawnienia użytkownika do systemu przetwarzającego dane osobowe
9. Administrator Systemu i Sieci rejestruje wykonane czynności w dziennikach systemu przetwarzania.
10. Identyfikatory użytkowników posiadających uprawnienia administracyjne przyznawane są na podstawie wniosku Administratora Bezpieczeństwa Informacji.
11. W systemie komputerowym istnieje konto w pełni administracyjne, którego można w sytuacjach awaryjnych użyć podczas nieobecności Administratora Systemu i Sieci. Dane tego konta Administrator Systemu i Sieci złożył w pok. nr 10C – Biuro Kierownika Zarządu, w szafie zamykanej na klucz w zamkniętej i opieczętowanej kopercie.
12. Osobami uprawnionymi do użycia specjalnego konta administracyjnego, o którym mowa w powyższym punkcie są Administrator Danych Osobowych lub osoby przez niego wyznaczone.
13. W przedsiębiorstwie prowadzi się ewidencję osób upoważnionych do przetwarzania danych osobowych (**załącznik nr 11**).
14. Dokumentację w formie załączników, o których mowa w niniejszym paragrafie zobowiązany jest prowadzić Administrator Bezpieczeństwa Informacji.

§2

STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA

1. W systemie komputerowym użytkownik identyfikowany jest jako obiekt o nazwie imie.nazwisko@mzgkns.local.
2. W zależności od poziomu uprawnień nadanych przez ABI Administrator Systemu i Sieci nadaje uprawnienia NTFS do katalogów konkretnych systemów przetwarzania danych osobowych.
3. System komputerowy raz na 30 dni blokuje konto użytkownika i podczas nowego logowania się do sieci wymusza zmianę hasła. O konieczności zmiany hasła system informuje 7 dni przed planowanym zablokowaniem konta.
4. System posiada zaimplementowany mechanizm uniemożliwiający użycie ostatnich 20 haseł
5. System wymusza użycie zasad złożoności hasła. W związku z 'wysokim poziomem zabezpieczeń' w sieci lokalnej ustala się, że hasło składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry i znaki specjalne.
6. W aplikacjach służących do przetwarzania danych osobowych stosowane jest uwierzytelnianie użytkownika przy pomocy jego identyfikatora i hasła.
7. Ze względu na różnorodność używanych w Przedsiębiorstwie aplikacji do przetwarzania danych osobowych nie można jednoznacznie zunifikować nomenklatury identyfikatorów. Identyfikator najbardziej pożądany to forma '*imie.nazwisko*'.
8. Każdy użytkownik systemu przetwarzania posiada swój unikalny identyfikator.
9. Użytkownicy nie mogą używać tych samych identyfikatorów, ani wymieniać się identyfikatorami.
10. Przy tworzeniu identyfikatora użytkownika Administrator Systemu i Sieci ustawia losowe hasło i przekazuje to hasło w formie pisemnej użytkownikowi.
11. Użytkownik jest zobowiązany zmienić hasło przy pierwszym dostępie do systemu lub aplikacji.
12. Hasło ważne jest maksymalnie 30 dni, po tym czasie powinno zostać zmienione. Jeśli aplikacja na to pozwala należy użyć mechanizmu automatycznej zmiany hasła, jeśli nie, to użytkownik jest zobowiązany pamiętać, aby raz na 30 dni zmienić hasło.
13. Każdy użytkownik zarządza swoimi hasłami dla wszystkich identyfikatorów, których używa.
14. Użytkownicy są zobowiązani do przestrzegania reguł odnośnie długości i złożoności hasła oraz okresu jego wymiany.
15. Hasło użytkownika jest jego własnością i zna je wyłącznie dany użytkownik. Zabronione jest przekazywania hasła innym osobom.
16. Niedopuszczalne jest podglądanie haseł wprowadzanych do systemu przez innych użytkowników. Jeżeli użytkownik w pobliżu zaczyna wprowadzać hasło należy odwrócić wzrok.
17. Hasło użytkownika jest składowane w systemie przetwarzania w bezpieczny sposób.
18. Hasło użytkownika nie jest pokazywane na ekranie lub wydrukach w postaci otwartego tekstu .
19. Hasło użytkownika nie może być przesyłane przez sieć otwartym tekstem.
20. Użycie konta, o którym mowa w par. 1 pkt. 11 niniejszej Instrukcji powinno zostać odnotowane w dzienniku logowania awaryjnego (**załącznik nr 6**). Ewidencję taką zobowiązany jest prowadzić ABI.

§3.

PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU

1) Przed rozpoczęciem pracy użytkownik powinien sprawdzić, czy stan sprzętu komputerowego nie wskazuje na próbę uruchomienia komputera przez osobę niepowołaną.
2) Monitory komputerów, na których przetwarza się dane, należy ustawiać tak, aby mogli z nich czytać wyłącznie Użytkownicy Danych Osobowych.
3) Po załadowaniu systemu operacyjnego wyświetli się okno logowania do systemu Windows, Użytkownik zostanie poinformowany przez system o konieczności wywołania pól informacyjnych używając kombinacji klawiszy CTRL+ALT_DEL
4) Aby zarejestrować się w systemie użytkownik musi w odpowiednie pola wpisać swój identyfikator, hasło oraz nazwę organizacji (domeny), do której się loguje.
5) Jeśli logowanie do systemu komputerowego przebiega po raz pierwszy użytkownik zostanie poproszony o zmianę hasła poprzez wypełnienie formularza, w którym podaje aktualne hasło, nowe hasło, które weryfikuje poprzez podwójne wpisanie w formularzu. Po zatwierdzeniu zmian następuje logowanie na nowym haśle.
6) Jeśli logowanie do systemu nie przebiegło pomyślnie, tzn. system komunikuje o błędnym loginie lub haśle należy sprawdzić, czy wyłączony jest klawisz CapsLock, włączona klawiatura numeryczna, zwrócić uwagę na użycie małych i dużych liter w haśle, sprawdzić czy użytkownik loguje się do właściwej domeny.
7) Dziesięciokrotne błędne wpisanie danych autentykacyjnych powoduje zablokowanie konta na okres 15 minut. O blokadzie konta użytkownik powiadamia Administratora Bezpieczeństwa Informacji.
8) Konto może odblokować ASiS na wniosek ABI (**załącznik nr 7**). Jednak zanim ABI taki wniosek sporządzi sprawdzi, czy nie doszło do przekroczenia uprawnień
9) Po odblokowaniu konta ASiS ustala nowe losowe hasło do konta i przekazuje je w formie pisemnej użytkownikowi. Użytkownik zobowiązany jest zmienić hasło niezwłocznie po zalogowaniu do systemu.
10) Po uruchomieniu systemu operacyjnego użytkownik użyje skrótów do właściwych sobie aplikacji przetwarzających dane osobowe.
11) Użytkownicy uzyskują bezpośredni dostęp do danych w aplikacji po wpisaniu w oknie autentykacji właściwego identyfikatora i hasła.
12) W czasie przerwy w korzystaniu z komputera z ekranu monitora powinien wyświetlać się na nim wygaszacz ekranu, którego odblokowanie wymaga podania hasła użytkownika.
13) Wygaszacz ekranu, o którym mowa w pkt. 12 włącza się po upływie 15 min od ostatniej czynności wykonanej przez użytkownika. W przypadku opuszczenia pokoju, w celu zabezpieczenia komputera przed dostępem osób niepowołanych należy zastosować kombinację klawiszy Windows+L.
14) Kończąc prace użytkownik powinien:
    a) wykonać kopie awaryjną (zapasową) z poziomu aplikacji do przetwarzania danych
    b) zamknąć program oraz wylogować się z systemu i wyłączyć komputer wraz z drukarką
    c) sprawdzić, czy na drukarce nie zostały żadne wydruki mogące zawierać dane osobowe.
15) Wszystkie zauważone nieprawidłowości na stanowisku użytkownik winien natychmiast zgłosić informatykowi oraz Administratorowi Bezpieczeństwa Informacji.

§4.

PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

1. Zabezpieczenia w postaci kopii zapasowych wymagają wszystkie zbiory opisane w par. 2 Polityki Bezpieczeństwa, a także systemy użyte do ich przetwarzania.

2. Kopie zapasowe wykonywane będą na dyskach HDD oraz taśmach magnetycznych przy użyciu systemowego programu Ntbackup lub podobnych. Kopiowanie na taśmy magnetyczne odbywa się przy użyciu streamera. Kopie baz danych tworzone będą przy użyciu tzw. job'ów administracyjnych, lub skryptów.

3. Harmonogram wykonywania kopii zapasowych.

Nr	Dzień tygodnia	Godzina	Rodzaj kopii	Nazwa pliku kopii	Ważny	Typ nośnika
1	Niedziela	14:00	Normalna	X_MC.bkf	4 miesiące	Taśma DAT
2	Niedziela	10:00	Normalna	x_TY.bkf	4 tygodnie	Taśma DAT
3	Niedziela	20:00	Normalna	0_ND.bkf	7 dni	HDD (k:\)
4	Poniedziałek	20:00	Przyrostowa	1_PN.bkf	7 dni	HDD (k:\)
5	Wtorek	20:00	Przyrostowa	2_WT.bkf	7 dni	HDD (k:\)
6	Środa	20:00	Przyrostowa	3_SR.bkf	7 dni	HDD (k:\)
7	Czwartek	20:00	Przyrostowa	4_CZ.bkf	7 dni	HDD (k:\)
8	Piątek	20:00	Przyrostowa	5_PT.bkf	7 dni	HDD (k:\)

4. Ustala się, że całkowity czas żywotności nośników użytych do przechowywania kopii zapasowych nie będzie dłuższy niż:

   a. 3 lata w przypadku dysków HDD

   b. 1 rok w przypadku dysków CD i DVD

   c. 10 lat w przypadku taśm magnetycznych (przy czym nie więcej niż ilość maksymalnej ilości nagrań określonej przez producenta taśmy).

5. Po wycofaniu z obiegu nośniki użyte do przechowywania kopii zapasowych powinny zostać zniszczone lub uszkodzone tak, aby nie można było odczytać z nich żadnych informacji. Przykładowo taśmę magnetyczną należy spalić, a dysk HDD można przewiercić wielokrotnie na wylot wiertłem.

6. W przypadku awarii dysku, który jest na gwarancji, serwis podczas przyjęcia dysku do naprawy ma obowiązek podpisać oświadczenie o zachowaniu w tajemnicy danych zawartych na uszkodzonym dysku. Wzór takiego oświadczenia stanowi **załącznik nr 12** do niniejszego dokumentu.

7. Osobą odpowiedzialną za wykonanie kopii zapasowych jest Administrator Systemu I Sieci.

§5.

SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA:

1) **Elektroniczne nośniki informacji** zawierające dane osobowe są częścią komputera, który je serwuje w sieci, dlatego znajdują się w serwerowni.
2) Pomieszczenie serwerowni posiada drzwi z zamkiem zamykanym na klucz, do którego dostęp posiada wyłącznie Administrator Bezpieczeństwa Informacji. Dostęp do pomieszczenia obligatoryjnie nabywa osoba będąca Administratorem Systemu i Sieci.
3) **Kopie zapasowe**, o których mowa w par. 3 poz. 2 oraz 3 do 8 – miejscem przechowywania jest serwerownia.
4) **Kopie zapasowe**, o których mowa w par. 3 poz. 1 – miejscem przechowywania kopii zapasowych z każdego miesiąca jest szafa zamykana na klucz, do której dostęp ma tylko Kierownik COŚ, w budynku Centralnej Oczyszczalni Ścieków.
5) Nośniki informatyczne, kopie awaryjne, o których mowa w ust. 4, przechowywać należy w wyznaczonych pomieszczeniach, w zamkniętych szafach.
6) Żywotność kopii zapasowych, o których mowa w par. 3 poz.3 wynosi **7 dni**. Siódmego dnia cyklu plik jest nadpisywany nowym plikiem kopii zapasowej.
7) Żywotność kopii zapasowych, o których mowa w par. 3 poz.2 wynosi 4 **tygodnie**. W ostatnią niedzielę najstarszy plik cyklu jest nadpisywany nowym plikiem kopii zapasowej z tygodnia.
8) Żywotność kopii zapasowych, o których mowa w par. 3 poz.1 wynosi **4 miesiące**. Pierwszego miesiąca nowego cyklu najstarsza taśma w zbiorach zostanie nadpisana nowym plikiem kopii zapasowej.
9) Za wydruki zawierające dane osobowe odpowiedzialni są Użytkownicy Danych Osobowych, którzy je wykonali.

§6

SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

1. Wyróżnia się kilka podstawowych kanałów implantacji szkodliwego oprogramowania do systemu komputerowego:
   1) Pobranie i/lub otwarcie 'zainfekowanego' załącznika poczty elektronicznej
   2) Uruchomienie 'zainfekowanego' pliku bezpośrednio ze strony internetowej (poprzez kliknięcie w link do niej, lub wpisanie adresu w przeglądarce) lub uruchomienie niepożądanego oprogramowania poprzez wyświetlenie 'zainfekowanego' obrazka lub zdjęcia na stronie internetowej
   3) Instalacja różnego rodzaju oprogramowania użytkowego lub gier itp., do którego dołączone jest niepożądane oprogramowanie
   4) Uruchomienie zawartości nośników zewnętrznych takich jak płyty CD i DVD, dyski 1,44'', przenośne urządzenia USB typu pendrive, karty pamięci, zewnętrzne dyski twarde a nawet telefony i urządzenia typu MP3.
   5) Włamanie do logicznej struktury sieci komputerowej
   6) Włamanie do fizycznej struktury sieci komputerowej
   7) Świadome, złośliwe działanie użytkownika systemu.

2. Aby zminimalizować ryzyko wprowadzenia do systemu niepożądanego oprogramowania wprowadza się następujące zasady:
   1) Poczta elektroniczna
      a) Pocztę elektroniczną należy pobierać z serwerów pocztowych wyłącznie programem wskazanym przez ASiS (tutaj jest to Thunderbird). ASiS włącza w programie pocztowym funkcję pobierania wyłącznie nagłówków wiadomości, funkcję śledzenia wiadomości szpiegowskich i spamu, włącza funkcję umożliwiającą programowi antywirusowemu ingerencję w zawartość zainfekowanego pliku poczty.
      b) Użytkownik po uruchomieniu programu zobaczy wyłącznie tytuły i nadawców wiadomości. Jeśli ufa danej wiadomości (nadawcy) użytkownik klika w jej tytuł pobierając resztę zawartości z serwera.
      c) Jeżeli do wiadomości dołączony jest plik wykonywalny (.exe) zostanie automatycznie usunięty z poczty przez program antywirusowy.
      d) Jeżeli do wiadomości dołączony będzie plik z grafiką (zdjęcie, ikona) program zablokuje ich wyświetlenie na ekran. Dopiero świadoma ingerencja użytkownika (poprzez użycie właściwej opcji programu) może wyświetlić pełną zawartość wiadomości. Zaleca się aby nie wyświetlać dodatkowej zawartości wiadomości, chyba, że wiadomość taka jest bez tego nieodczytywalna.
      e) Zabrania się pobierania wiadomości z nagłówków o wątpliwej treści i od podejrzanych nadawców. Zabrania się otwierania jakichkolwiek plików dołączonych do takich e-maili. W przypadku otrzymania nagłówka wiadomości w języku, którego użytkownik nie rozumie i nic nie wskazuje, że jest to spam, użytkownik nie powinien pobierać reszty wiadomości. Należy poinformować ABI
      f) Jeżeli do wiadomości dołączony został plik, który jest nam potrzebny należy zapisać go do lokalizacji P:_pobieralnia a następnie jak najszybciej sprawdzić

oprogramowaniem antywirusowym. Należy pamiętać aby na bieżąco usuwać wiadomości, których treść przestała być aktualna.

2) Przeglądanie stron internetowych

a) Do przeglądania zawartości sieci publicznej Internet używać wyłącznie programu wskazanego przez ASiS (tutaj jest to Firefox). ASiS włącza w przeglądarce opcje zmniejszające ryzyko zainfekowania systemu niepożądanym oprogramowaniem.

b) Zabrania się przeglądania serwisów, które nie służą powierzonym pracownikowi zadaniom służbowym, szczególnie należy tu wskazać serwisy o wątpliwej treści z naciskiem na serwisy gier i erotyczne.

c) Pliki są pobierane przez Firefoxa do folderu P:_pobieralnia gdzie powinny zostać przeskanowane pod kątem antywirusowym niezwłocznie po zakończeniu ich pobierania.

d) Zabrania się przenoszenia lub kopiowania pobranych z Internetu plików z dysków lokalnych komputera na dyski sieciowe bez absolutnej pewności co do ich nieszkodliwości.

3) Oprogramowanie

a) Zabrania się samodzielnego instalowania oprogramowania komputerowego. Osobą odpowiedzialną za instalację oprogramowania jest ASiS.

b) ASiS przed pierwszym zainstalowaniem programu na systemie produkcyjnym najpierw przetestuje jego działanie na systemie testowym sprawdzając także pod kątem antywirusowym.

c) Wiele szkodliwych programów instaluje się poprzez udawanie programu antywirusowego. Na ekranie monitora pojawiają się wtedy alarmujące ostrzeżenia o zainfekowaniu systemu i oferta jego wyleczenia, wg której wystarczy kliknąć w wyświetlony link, aby zapobiec zagrożeniu. Pod żadnym pozorem nie można tego robić!!!. Należy poinformować ASiS lub informatyka.

4) Nośniki informacji

a) Zabrania się używania jakichkolwiek zewnętrznych nośników informacji. W tym celu ASiS blokuje taką możliwość w systemie komputerowym.

b) wydziela się 1 stanowisko komputerowe w Przedsiębiorstwie (dodatkowy komputer w sekretariacie), tzw. Stanowisko Wymiany Danych, na którym będzie można wymieniać informacje z nośników zewnętrznych. Stanowisko to nie jest podłączone do jakiejkolwiek sieci.

c) Osobą obsługującą Stanowisko Wymiany Danych jest zapoznana z ustawą o ochronie danych osobowych i przeszkolona w zakresie obsługi zainstalowanego na nim oprogramowanie antywirusowego w stopniu minimum podstawowym.

d) W przypadku potrzeby zgrania danych z nośnika zewnętrznego, należy wyświetlić jego zawartość i konkretny plik lub folder przeskanować oprogramowaniem antywirusowym.

e) Zabrania się używania nośników zewnętrznych, np. typu pendrive, które do uruchomienia lub wyświetlenia zawartości wymagają praw administracyjnych (np. pendrive zabezpieczony hasłem, które wymaga uruchomienia z uprawnieniami administracyjnymi aplikacji do weryfikacji haseł)

f) W przypadku pozytywnego rezultatu skanowania antywirusowego należy niezwłocznie odłączyć zewnętrzny nośnik danych (np. wyjąć pendrive, wyjąć płytę DVD z napędu) a następnie uruchomić pełne skanowanie antywirusowe systemu i powiadomić ABI.

g) W przypadku rezultatu negatywnego pożądaną zawartość należy zgrać na dysk lokalny komputera i odłączyć zewnętrzny nośnik danych.

h) Jeżeli to możliwe należy uruchomić zgraną zawartość w celach testowych.

i) Jeżeli osoba obsługująca stanowisko nie wniesie żadnych zastrzeżeń co do zawartości zgranych plików może je przenieść do sieci lokalnej używając do tego służbowego pendrive'a.
j) Pendrive służbowy po każdym użyciu powinien zostać sformatowany.
k) Zabrania się nagrywania na pendive informacji podczas gdy znajdują się na nim inne pliki. W takim przypadku przed nagraniem należy sformatować pendrive.

5) Połączenie do sieci publicznej

a) System łączy się z siecią publiczną za pośrednictwem komputera pełniącego funkcję routera i firewall (tzw. brama).
b) System operacyjny takiego komputera powinien być jak najbardziej odporny na ataki, zalecany UNIX (tutaj: *FreeBSD* z firewall-em *OpenBSD PF Firewall*)
c) Lista dostępnych portów i usług, które oferuje brama, stanowi **załącznik nr 8** do niniejszej instrukcji
d) Dostęp zdalny z sieci publicznej do sieci lokalnej realizowany jest poprzez protokół VPN. Użytkownik na **załączniku nr 9** wnioskuje do ABI o przyznanie zdalnego dostępu, a ten wnioskuje do ASiS o wydanie certyfikatu VPN, bez którego nie jest możliwy dostęp zdalny.
e) Certyfikat ważny jest na czas określony we wniosku, nie dłuższy niż 3 miesiące. Po tym czasie należy wystąpić z wnioskiem o nowy certyfikat.
f) Zdalny dostęp do sieci lokalnej możliwy jest wyłącznie z urządzeń będących pod jurysdykcją aktualnego ASiS (czyli nie można dostać się do sieci z komputerów np. w kawiarence internetowej, lub prywatnego sprzętu pracownika)

6) Dostęp nieupoważniony.

a) Zabrania się przebywania osobom nieupoważnionym bez obecności Pracownika w pomieszczeniach, w których znajdują się podłączone do sieci lokalnej komputery.
b) Po godzinach urzędowania budynek jest zamykany i sprzątany. Zabrania się osobom sprzątającym włączania jakichkolwiek urządzeń komputerowych.
c) Zabrania się osobom sprzątającym wpuszczania do budynku osób nieupoważnionych.
d) Po zakończeniu wszelkich prac budynek jest zamykany na klucz. Włączony zostaje system alarmowy, który w razie włamania uruchamia syrenę i powiadamia firmę ochroniarską.
e) Po godzinach urzędowania w budynku lub na terenie Zakładu znajduje się osoba z firmy ochroniarskiej.

7) Serwer

a) Zakupiony i wdrożony przez Przedsiębiorstwo system komputerowy Microsoft Windows Smal Business Server 2003 R2 zapewnia możliwość takiej jego konfiguracji, aby użytkownicy mieli uprawnienia do pracy w systemie na takim poziomie, jaki uznał ABI w stosownych dokumentach (**załączniki 1 i 2**). Jednostką odpowiedzialną za tą konfigurację jest Administrator Systemu i Sieci.
b) System automatycznie po nazwie rozpoznaje prawa użytkownika. Tylko użytkownicy z uprawnieniami administracyjnymi (w tym ASiS, konto awaryjne) mogą instalować i uaktualniać aplikacje. Zwykły użytkownik domeny podczas próby instalacji jakiegokolwiek programu otrzyma komunikat z systemu informujący go, że nie ma praw do tej operacji.

c) Każdy użytkownik mający dostęp do sieci podpisuje stosowne oświadczenie o zachowaniu poufności danych, stanowiące **załącznik nr 3** do niniejszej Instrukcji.

8) Oprogramowanie antywirusowe.

a) W systemie komputerowym zaimplantowano tak na serwerze jak i na stacjach roboczych system antywirusowy DrWeb, który pozwala na skanowanie w czasie rzeczywistym plików i procesów działających w systemie a także skanuje pocztę wchodzącą i wychodzącą z programów pocztowych. Program antywirusowy oferuje ewidencję zdarzeń z ostatnich 12 miesięcy.

b) Sygnatury wirusów i uaktualnienia programu antywirusowego pobierane są:
   1. Na serwerze: każdego dnia w godzinach nocnych narzędzie aktualizacji uruchamiane jest przez program.
   2. Użytkownik włączając swój komputer uruchamia także procedurę aktualizacyjną

c) Raz w tygodniu przeprowadza się automatycznie pełne skanowanie systemów zarówno serwera jak i systemów klienckich. Automat ustawiony jest na usuwanie zainfekowanych plików i powiadamianie ASiS o infekcji.

d) Komunikat DrWEB o wykryciu infekcji w trybie on-line: użytkownik powinien użyć funkcji usunięcia pliku jeśli taka jest dostępna. Jeśli opcji takiej nie ma, lub jest ona niedostępna należy wybrać opcję wyleczenia lub zablokowania pliku. Nigdy nie należy używać opcji ***ignoruj***! Należy niezwłocznie odłączyć komputer od sieci komputerowej poprzez wyjęcie kabla z gniazda i poinformować o tym fakcie ASiS lub informatyka. Nie podłączać komputera do sieci komputerowej do czasu wyraźnej zgody tych osób.

§7

SPOSOBY ODNOTOWANIA INFORMACJI O ODBIORCACH DANYCH OSOBOWYCH

1. Każdy program do przetwarzania danych osobowych powinien posiadać swój dziennik odbiorców tych danych. Dziennik taki prowadzony jest przez właściwych Użytkowników Danych Osobowych.
2. Dziennik zawiera datę i zakres udostępnionych danych oraz dane identyfikujące odbiorcę.
3. Na dane o odbiorcach danych osobowych składają się:
    a. Imię
    b. Nazwisko
    c. PESEL
4. Dziennik prowadzi się także w formie papierowej, która stanowi **załącznik nr 10**.

PREZES ZARZĄDU

Waldemar Wrześniak

Załącznik nr 1

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Udzielam upoważnienia do przetwarzania danych osobowych dla:

1. Imię: .....

2. Nazwisko: .....

3. Stanowisko służbowe: .....

4. Pełna nazwa Wydziału: .....

5. Okres obowiązywania upoważnienia (proponowany) od .....do .....

W nw. zakresie:

Lp.	Zbiór danych	Systemy informatyczne[1]	Uprawnienia[2]	Uprawnienia[3]	Uprawnienia[3]	IDENTYFIKATOR (LOGIN)	Hasło[4]
				Zapis	Odczyt	wypełnia Administrator Systemu i Sieci	
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							

[1] systemy informatyczne korzystające z danego zbioru danych

[2] uprawnienia – w przypadku ubiegania się o nadanie uprawnienia wpisz „TAK", w przeciwnym przypadku wpisz „NIE" dla odpowiedniego zbioru danych osobowych.

[3] Wypełnia Administrator Bezpieczeństwa Informacji

[4] zmienić natychmiast przy pierwszym logowaniu do systemu

Nowa Sól, dnia ....

(*czytelny podpis Administratora Danych Osobowych*)

Nadany numer upoważnienia: _____

Załącznik nr 2

WNIOSEK O ZAŁOŻENIE KONTA
W SYSTEMIE INFORMATYCZNYM PRZEDSIĘBIORSTWA

Wnioskuję o założenie konta w systemie informatycznym MZGK Sp. z o.o. w Nowej Soli dla:

1. Imię: .....

2. Nazwisko: .....

3. Stanowisko służbowe: .....

4. Pełna nazwa Wydziału: .....

5. Okres obowiązywania upoważnienia (proponowany) od ..... do .....

6. Zakres uprawnień (postawić znak X we właściwym wierszu, ostatnią kolumnę wypełnia ABI)

X	Użytkownik domeny	
	Administrator	
	Administrator domeny	
	Administrator przedsiębiorstwa	
	Administrator schematu	
	Mobile User	
	Twórca – właściciel zasad grupy	

Nowa Sól, dnia ....
(*czytelny podpis osoby zgłaszającej wniosek*)

W dniu ..... w systemie informatycznym MZGK Sp. z o.o. w Nowej Soli założono konto o:

identyfikatorze: .....@mzgkns.local

z hasłem:.....które należy zmienić podczas pierwszego logowania do systemu.

Nowa Sól, dnia ....
(*czytelny podpis Administratora Systemu i Sieci*)

Załącznik nr 3

1. Imię: .....

2. Nazwisko: .....

3. Stanowisko służbowe: .....

OŚWIADCZENIE O POUFNOŚCI DANYCH

1. Zobowiązuję się do bezwzględnego zachowania w tajemnicy wszelkich informacji uzyskanych w związku z wykonywaniem umowy, także po zakończeniu realizacji umowy. Obowiązek ten nie dotyczy informacji co, do których MZGK Sp. z o.o. w Nowej Soli ma nałożony ustawowy obowiązek publikacji lub która stanowi informacje jawną, publiczną opublikowaną przez MZGK Sp. z o.o. w Nowej Soli.
2. W przypadku naruszenia zapisów ustawy o ochronie danych osobowych MZGK Sp. z o.o. w Nowej Soli może wypowiedzieć umowę ze skutkiem natychmiastowym.

Nowa Sól, dnia ....

(czytelny podpis osoby składającej oświadczenie)

Załącznik nr 4

WNIOSEK O
BLOKADĘ/USUNIĘCIE KONTA
W SYSTEMIE INFORMATYCZNYM PRZEDSIĘBIORSTWA

Proszę o blokadę/usunięcie* konta w systemie informatycznym MZGK Sp. z o.o. w Nowej Soli dla:

1. Imię: .....

2. Nazwisko: .....

3. Okres obowiązywania blokady do dnia .....

4. Powód blokad/usunięcia .....

.....

** niepotrzebne skreślić*

Nowa Sól, dnia ....
(*czytelny podpis osoby ABI*)

W dniu ..... w systemie informatycznym MZGK Sp. z o.o. w Nowej Soli zablokowano/usunięto konto o ww. identyfikatorze.

.....
(*czytelny podpis Administratora Systemu i Sieci*)

Załącznik nr 5

ZMIANA UPRAWNIEŃ W SYSTEMIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Proszę o zmianę uprawnień dla:

1. Imię: .....

2. Nazwisko: .....

3. Dotyczy upoważnienia nr: .....

Lp.	Zbiór danych	Systemy informatyczne[1]	Uprawnienia[2]		UWAGI
			Zapis	Odczyt	
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					

[1] systemy informatyczne korzystające z danego zbioru danych
[2] Wypełnia Administrator Bezpieczeństwa Informacji

Upoważniam wskazaną osobę do przetwarzania danych osobowych w wyżej opisanym zakresie.

Nowa Sól, dnia ....
(*czytelny podpis Administratora Bezpieczeństwa Informacji*)

W dniu ..... w systemie informatycznym MZGK Sp. z o.o. w Nowej Soli zmieniono uprawnienia ww. użytkownika systemu w zakresie opisanym w powyższej tabeli.

.....
(*czytelny podpis Administratora Systemu i Sieci*)

Ewidencja logowań kontem awaryjnym

Załącznik nr 6

Lp	data	godzina logowania	godzina wylogowania	osoba logująca	cel logowania	uwagi
1						
2						
3						
4						
5						
6						
7						
8						

Załącznik nr 7

WNIOSEK O ODBLOKOWANIE KONTA
W SYSTEMIE INFORMATYCZNYM PRZEDSIĘBIORSTWA

Wnioskuję o odblokowanie konta w systemie informatycznym MZGK Sp. z o.o. w Nowej Soli dla:

1. Imię:.....

2. Nazwisko: .....

Nowa Sól, dnia ....
(czytelny podpis osoby zgłaszającej wniosek)

Nowa Sól, dnia ..... AKCEPTUJĘ.....
(czytelny podpis ABI)

W dniu ..... w systemie informatycznym MZGK Sp. z o.o. w Nowej Soli odblokowano konto o:

identyfikatorze: .....@mzgkns.local

z hasłem:.....które należy zmienić podczas pierwszego logowania do systemu.

Nowa Sól, dnia ....
(czytelny podpis Administratora Systemu i Sieci)

Załącznik nr 8

LISTA DOSTĘPNYCH USŁUG I OTWARTYCH PORTÓW, KTÓRE OFERUJE BRAMA

Lp	Nazwa protokołu / usługi	PORT	UWAGI
1	Remote Desktop	3388	
2	OpenVNC		
3	FTP	20, 21, 1024	
4	SSH	22	
5	SMTP	25	
6	POP3	110	

Załącznik nr 9

WNIOSEK O ZDALNY DOSTĘP DO SIECI KOMPUTEROWEJ MZGK Sp. z o.o. w Nowej Soli

Wnioskuję o zdalny dostęp do sieci komputerowej MZGK Sp. z o.o. w Nowej Soli dla:

1. Imię: .....

2. Nazwisko: .....

3. Stanowisko służbowe: .....

4. Pełna nazwa Wydziału: .....

5. Okres obowiązywania dostępu (proponowany) od ..... do .....

Nowa Sól, dnia ....
(*czytelny podpis osoby zgłaszającej wniosek*)

Nowa sól, dnia ..... AKCEPTUJĘ.....
(*czytelny podpis ABI*)

W dniu ..... wygenerowano i wgrano na system kliencki certyfikat dostępu zdalnego VPN:

Nazwa pliku:.....

Okres ważności certyfikatu.....

Nowa Sól, dnia ....
(*czytelny podpis Administratora Systemu i Sieci*)

Ewidencja danych udostępnionych

Załącznik nr 10

Lp	data	ODBIORCA danych				Osoba, której dotyczą udostępnione dane osobowe			UWAGI
		Imię	Nazwisko	PESEL	Nr dowodu osobistego	Imię	Nazwisko	PESEL	
1									Udostępnił:
zakres udostępnionych danych:									
2									Udostępnił:
zakres udostępnionych danych:									
3									Udostępnił:
zakres udostępnionych danych:									
4									Udostępnił:
zakres udostępnionych danych:									
5									Udostępnił:
zakres udostępnionych danych:									

Załącznik nr 11

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Lp	imię	Nazwisko	data nadania upoważnienia	data ustania upoważnienia	zakres upoważnienia	identyfikator w systemie informatycznym	identyfikator w programie do przetwarzania danych
1							
2							
3							
4							
5							
6							
7							
8							

Załącznik nr 12

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH W SERWISIE TECHNICZNYM

Udzielam upoważnienia do przetwarzania danych osobowych dla:

Nazwa firmy lub pieczęć firmowa:

Na czas konieczny do naprawy urządzenia, na którym przechowuje się dane osobowe.
WW firma oświadcza, że zachowa w tajemnicy informacje, które:

a) stanowią tajemnicę przedsiębiorstwa
b) są danymi osobowymi
c) nabyte od osoby nieuprawnionej zagrażają lub naruszają interes przedsiębiorcy.

Przez tajemnicę przedsiębiorstwa rozumie się nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności.

Nowa Sól, dnia ....
(*czytelny podpis osoby przekazującej urządzenie do naprawy*)

....., dnia ....
(*czytelny podpis osoby przyjmującej urządzenie do naprawy*)