

**SPRAWOZDANIE Z KONTROLI RADY NADZORCZEJ
W SPÓŁCE „MIEJSKIE WODOCIĄGI I KANALIZACJA”
SPÓŁKA Z O. O. W KOŁOBRZEGU
ZA I PÓŁROCZE 2014 ROKU**

Rada Nadzorcza w oparciu o Regulamin przeprowadzania kontroli przez Radę Nadzorczą w Spółce MWiK Sp. z o. o. w Kołobrzegu, stanowiący załącznik Nr 1 do Uchwały Nr 22/2008 Rady Nadzorczej „Miejskich Wodociągów i Kanalizacji” Sp. z o. o. w Kołobrzegu z dnia 08.07.2008 roku, przeprowadziła kontrolę zgodnie z planem kontroli, stanowiącym załącznik do Uchwały Nr 1/2014 z dnia 31.01.2014 r. Rady Nadzorczej.

Kontrolę przeprowadzono w okresie: maj 2014 r. – czerwiec 2014 r.

Kontrolą objęto **Dział Informatyczny MWiK w Kołobrzegu**. Zakres kontroli obejmował następujące obszary:

- 1) Analiza stanu sprzętu informatycznego (hardware) MWiK.
- 2) Analiza stanu oprogramowania (software) MWiK.
- 3) Ocena wykorzystywania sprzętu komputerowego przez pracowników MWiK, w szczególności:
 - a) możliwość korzystania w czasie godzin pracy przez pracowników z portali społecznościowych,
 - b) formy komunikacji komputerowej wewnętrznej,
 - c) korzystanie przez pracowników z urządzeń „zewnętrznych” (pendrive, przenośne dyski twarde itp.),
 - d) wykorzystywanie nielegalnego oprogramowania na sprzęcie MWiK (programy bez licencji, programy nie będące własnością MWiK).
- 4) Sposoby likwidowania sprzętu komputerowego i oprogramowania.
- 5) Stan zaawansowania prac wdrożeniowych firmy UNISOFT.
- 6) Planowane zakupy oprogramowania i sprzętu komputerowego oraz źródła ich finansowania,
- 7) Dostęp klientów do systemu informatycznego MWiK.

Kontrolującym był:

1. Przewodniczący Rady Nadzorczej – Edward Wiśniewski

SZCZEGÓŁOWE CZYNNOŚCI KONTROLNE:

1. ANALIZA STANU SPRZĘTU INFORMATYCZNEGO MWIK

Aktualny stan posiadania sprzętu informatycznego Spółki jest następujący:

- a) 68 komputerów (*deskopów*) o zróżnicowanym stanie technicznym: 25 – stan dobry, 25 – stan dostateczny, 18 – stan zły (do likwidacji),
- b) 15 *laptopów*: 10 – stan dobry, 5 – stan dostateczny,
- c) 6 *serwerów*: 2 – stan bardzo dobry, 1 – stan dobry, 1 – stan dostateczny, 1 – do likwidacji.

Szczegółowy wykaz sprzętu zawierają Zał. 1 i Zał.2. Serwis techniczny komputerów jest realizowany systematycznie przez Dział NI MWiK. Konserwacje i naprawy uszkodzonych monitorów oraz drukarek realizują w systemie outsourcing firmy zewnętrzne. Średnia ilość zleceń zewnętrznych kształtuje się na poziomie 20 – 25 zleceń rocznie.

2. ANALIZA STANU OPROGRAMOWANIA MWIK

Struktura oprogramowania na stanie Spółki jest następująca:

- a) *oprogramowanie systemowe*: 61 licencji Microsoft Windows XP, 2 licencje Microsoft Vista, 21 licencji Microsoft 7, 2 licencje Windows Server 2008, 1 licencja Microsoft Windows Server 2000, 1 licencja Suse Linux Enterprise Server 10, 1 licencja Novell Netware 5.0,
- b) *oprogramowanie biurowe*: 53 licencji Microsoft Office, 10 licencji Open Office, 15 licencji Libre Office,
- c) *oprogramowanie antywirusowe*: 50 licencji Comodo Internet Security, 10 licencji Herosoft, 26 licencji Ms Security Essentials.
[Zał. 3, Zał. 4, Zał. 5].
- d) *oprogramowanie użytkowe (aplikacje)*: wykorzystywany jest Zintegrowany System Informatyczny (ZSI) firmy UNISOFT. W skład systemu wchodzi następujące moduły:
 - d1) z zakresu ewidencyjno- sprawozdawczego: Finansowo-Księgowy (F-K), Majątek Trwały, Obrót towarowo-materiałowy, Kadry i płace,
 - d2) z zakresu zarządzania Spółką: Zarządzanie i planowanie, Zarządzanie infrastrukturą, Zarządzanie obiegiem informacji, Transport i sprzęt, Zlecenia,
 - d3) z zakresu działalności podstawowej Spółki: Centrum informacji o kliencie, Należności i zobowiązania, Woda – system bilingowy.

[nie wszystkie z w/w modułów funkcjonują – trwają prace wdrożeniowe].

Na wyposażeniu informatycznym jest ponadto oprogramowanie do kompresji danych: 7zip oraz IZarc (oprogramowanie darmowe do użytku komercyjnego). Darmowe jest również oprogramowanie biurowe: Open Office, Libre Office oraz oprogramowanie antywirusowe. Pracownicy Działu NI kładą szczególny nacisk na używanie przez siebie darmowego oprogramowania diagnostycznego, oprogramowania serwisowego i wykonującego kopie zapasowe.

3. OCENA WYKORZYSTANIA SPRZETU I OPROGRAMOWANIA PRZEZ PRACOWNIKÓW MWIK

3.1. MOŻLIWOŚĆ KORZYSTANIA W CZASIE PRACY PRZEZ PRACOWNIKÓW Z PORTALI SPOŁECZNOŚCIOWYCH.

Kontrola ma na celu sprawdzenie możliwości dostępu pracowników w godzinach pracy do portali społecznościowych takich jak Nasza-klasa, Allegro itp. Z relacji pracownika NI Witolda Miśtaka wynika, że nie ma blokad formalnych. Istnieje problem techniczny: niedoskonałość urządzenia brzegowego – filtry nie potrafią odróżnić ciągu znaków od „zbitki literowej”, np. nk.pl (Nasza Klasa) a bank.agricole.pl. Ponieważ dotychczas producent nie naprawił tego problemu, w MWiK nie filtruje się stron, a jedynie monitoruje, co może wykryć incydentalne przypadki. Nie stwierdza się przekraczania ustalonych norm „wykorzystywania prywatnego”. Całkowite zablokowanie stron zewnętrznych jest możliwe poprzez blokowanie ustawień odpowiedzialnych za wyświetlanie określonych stron w przeglądarkach internetowych oraz blokowanie tych stron w routerze, ale nie jest to wskazane z uwagi na wykorzystywanie przez pracowników Internetu do celów służbowych. Często pracownicy w Internecie poszukują informacji z dziedziny ochrony środowiska, nowych technologii stosowanych na ujęciach wody czy oczyszczalni ścieków. Dział Zamówień wykorzystuje też portal Allegro do dokonywania zakupów lub porównywania cen poszukiwanych materiałów i urządzeń potrzebnych w danym momencie w Spółce. Ponadto realizowana jest komunikacja z jednostkami publicznymi, służbami technicznymi, inwestorami, projektantami oraz poszukiwanie ofert.

3.2. FORMY KOMPUTEROWEJ KOMUNIKACJI WEWNĘTRZNEJ - INTRANET

Główną formą komunikacji wewnętrznej jest poczta elektroniczna oraz wykorzystywanie zasobów sieciowych (dokumentacja). Informatyk Witold Miśtak poinformował, iż kilka lat temu zainstalował serwer komunikacyjny Jabber (bezpłatna licencja typu open source o nieograniczonym okresie ważności) do komunikacji wewnątrz Spółki. Nie było dużego zainteresowania ze strony pracowników tą formą

komunikowania się: ulokowanie komórek związanych z zarządzaniem w jednym budynku bardziej sprzyja przekazywaniu sobie informacji w formie ustnej.

3.3. KORZYSTANIE PRZEZ PRACOWNIKÓW Z URZADZEŃ ZEWNĘTRZNYCH

Kontrola ma na celu sprawdzenie możliwości kopiowania informacji będących w posiadaniu Spółki. Według relacji Informatyka NI nie było stwierdzonych faktów kopiowania informacji służbowych („wrażliwych” strategicznie, tj. dane odbiorców wody, dostawców ścieków, ich salda itp.). Tymczasem blokady jako takiej nie ma, aczkolwiek nie jest dla NI problem: można założyć blokady na porty USB, ale przy generalnym wykorzystywaniu poczty elektronicznej przez pracowników, dane można przysyłać e-mailem. Każdy z pracowników w momencie zatrudnienia podpisuje oświadczenie o zachowaniu tajemnicy służbowej (zachowanie w tajemnicy informacji pozyskanych w Spółce).

3.4. WYKORZYSTYWANIE NIELEGALNEGO OPROGRAMOWANIA

Kontrola miała na celu stwierdzenie faktów wykorzystywania sprzętu komputerowego do ściągania niepowołanych danych (filmy, muzyka itp.) i korzystania z oprogramowania nie będącego własnością Spółki lub nie posiadających wymaganej licencji (przeznaczenie komercyjne). Ponadto sprawdzenie zabezpieczenia sprzętu komputerowego przed instalowaniem niepowołanego oprogramowania lub treści multimedialnych.

Według Informatyka NI stwierdzono tego typu instalacje, mimo ograniczania kont użytkowników. Oprogramowanie każdorazowo usunięto, a z pracownikami przeprowadzono rozmowy informacyjno-uświadamiające. W ostatnim okresie brak takich zdarzeń. Wykryto proste programy do archiwizacji danych, proste przeglądarki plików graficznych: w mniemaniu użytkowników mają one status freeware, ale po analizie ich licencji przez Dział NI okazało się, że niektóre z nich mają ten status tylko do zastosowania domowego.

Okresowo lub wrywkowo prowadzone są kontrole legalności oprogramowania, zazwyczaj podczas przeglądów i napraw serwisowych. Zainstalowana jest również aplikacja o nazwie „Ewidencja sprzętu komputerowego i oprogramowania”, która na bieżąco rejestruje zmiany w konfiguracjach komputerowych. Jednakże oprogramowanie to nie posiada możliwości automatycznego wykrywania tych zdarzeń. Dysk wewnętrzny C i D są widoczne dla użytkownika i może sam bez wiedzy Informatyka dokonywać instalacji i usuwać oprogramowanie na komputerze.

Użytkownik nie ma też żadnych utrudnień w ściąganiu z sieci danych multimedialnych, co może narazić Spółkę na konsekwencje prawne oraz spowolnienie działania sieci internetowej.

4. SPOSOBY LIKWIDOWANIA SPRZĘTU KOMPUTEROWEGO I OPROGRAMOWANIA

Na podstawie druku LT (Likwidacja środków trwałych) wystawionego przez Dział NI oraz protokołu likwidacji sporządzanego na potrzeby Komisji Likwidacyjnej następuje „akt likwidacji”. Przed likwidacją sprzętu komputerowego następuje bezpowrotne zniszczenie danych zawartych na nośnikach wykorzystywanych poprzez komputer. Dyski twarde, karty pamięci oraz pendrive’y kasowane są bezpiecznymi algorytmami typu: Peter Gutmann, US DOD 5220.22-M, BSI S 2.167, Air Force System Security Instruction 5020, German Vsiotr. Ewentualne nośniki nie kasowane niszczone są mechanicznie. Obecnie Spółka nie ma podpisanej umowy dotyczącej odbioru i przetwarzania zużytego sprzętu elektrycznego i elektronicznego.

Jeżeli istnieje możliwość wykorzystania oprogramowania (względy licencyjne) z likwidowanego komputera, może ono zostać powtórnie zainstalowane. Oprogramowanie, którego ważność wygasła składowane jest w wydzielonym miejscu sejfów z nośnikami informatycznymi. Likwidację zatwierdza Komisja Likwidacyjna. Po zatwierdzeniu likwidacji urządzenia przekazywane są firmom utylizującym tego typu odpady.

Przeciętny czas wykorzystania sprzętu komputerowego w Spółce wynosi od 4 do 7 lat.

Spółka posiada oprogramowania o znacznej wartości, które jest na bieżąco wykorzystywane. W Spółce znajduje się wycofany ze względów uszkodzeń oraz „starości technologicznej” sprzęt komputerowy, który może być wykorzystywany jako swoisty magazyn części zamiennych.

5. STAN ZAAWANSOWANIA PRAC WDROŻENIOWYCH UNISOFT

Trwa proces wdrażania kompletnego Zintegrowanego Systemu Informatycznego firmy UNISOFT. Większość modułów jest wdrożona. Nie są w pełni wdrożone moduły: Zlecenia oraz Zarządzanie infrastrukturą. Uwagi w zakresie funkcjonowania modułów wdrożonych są na bieżąco uwzględniane i dokonuje się korekt i poprawek. Prace wdrożeniowe oraz korekcyjne nie wiążą się z dodatkowymi kosztami Spółki.

6. ZAKUPY SPRZĘTU KOMPUTEROWEGO I OPROGRAMOWANIA ORAZ ŹRÓDŁA ICH FINANSOWANIA

Pełna realizacja kontraktu z firmą UNISOFT powinna zabezpieczyć obsługę informatyczną Spółki w najbliższym okresie od strony oprogramowania. Naturalne zużywanie się sprzętu komputerowego może być uzupełniane zakupami bieżącymi ze środków własnych Spółki.

7. DOSTĘP KLIENTÓW DO SYSTEMU INFORMATYCZNEGO MWIK

Według relacji Informatyka NI na początku IV kwartału 2014 r. zostanie uruchomiony e-book MWIK w Kołobrzegu pod adresem:

[https:// ebok.mwik.kolobrzeg.pl](https://ebok.mwik.kolobrzeg.pl)

który będzie umożliwił klientom komputerowy dostęp do następujących informacji: dostęp do własnego konta, sprawdzenie salda na koncie, pobranie faktury w postaci dokumentu pdf, dokonanie płatności elektronicznej za zużytą wodę i odprowadzone ścieki, sprawdzenie stanu odczytów liczników, wprowadzenie własnego odczytu oraz korespondencja elektroniczna z MWIK (w tym reklamacje).

WNIOSKI POKONTROLNE:

1. Zaniepokojenie budzi jakościowa struktura posiadanych przez Spółkę komputerów: 26,5 % sprzętu jest do likwidacji, 37 % oceniono jako stan techniczny – dostateczny, 37 % jest w stanie dobrym, natomiast w zbiorze brakuje sprzętu bardzo dobrego.

Zaleca się w trybie pilnym dokonanie przez Dział NI „inwentaryzacji jakościowej” komputerów i przekazanie Zarządowi Spółki raportu w zakresie konieczności zakupu sprzętu bardzo dobrego (ilość, jakość, ceny).

Bieżące procesy informatyczne wymagają zabezpieczenia w dostateczną ilość nośników informacji (m.in. pendriv’y, papier do drukarek). Należy racjonalnie gospodarować nośnikami (ewidencja zużycia) pod nadzorem Działu NI.

2. Brak uwag i zaleceń.

3 a) Kontrolujący sugeruje wprowadzenie blokad dostępu do stron internetowych nie związanych z wypełnianiem obowiązków służbowych, a mogących być wykorzystywanymi przez pracowników Spółki w celach prywatnych np. portale społecznościowe np. Facebook czy internetowe zakupy/aukcje np. Allegro. Przyjęcie założenia, iż zdarzenia tego typu są incydentalne nie jest wystarczającym argumentem dla zabezpieczenia Spółki przed nieuzasadnionymi kosztami oraz łamaniem regulaminowych zasad pracy przez pracowników .

3 b) Zaleca się kontynuowanie prac zmierzających do zabezpieczenia sprzętu komputerowego Spółki i uniemożliwienia zgywania na wszelkiego rodzaju nośniki materiałów do których prawo przetwarzania i archiwizowania ma Spółka oraz uniemożliwienie kopiowania oprogramowania, do którego Spółka posiada licencje lub jest jego właścicielem.

3 c) Kontrolujący zaleca podjęcie próby zablokowania z poziomu użytkownika dostępu do dysku C i/lub D, możliwości instalacji na stacji roboczej niepowołanego oprogramowania oraz ściągania z sieci danych (w tym zdjęcia, muzyka, filmy). Stwierdzenie takich faktów przez instytucje kontroli zewnętrznej może doprowadzić do poniesienia przez Zarząd odpowiedzialności prawnej a Spółkę na straty finansowe z tytułu użytkowania „pirackich” programów lub archiwizowania treści multimedialnych bez posiadania do nich praw.

4. Brak uwag i zaleceń.
5. Respektować harmonogram prac wdrożeniowych od firmy UNISOFT.
6. Brak uwag i zaleceń do punktu.
7. Doprowadzić do skutecznego wdrożenia komputerowego systemu dostępu klienta do MWiK.

Zarząd Spółki ustosunkowując się do ww. wniosków pokontrolnych, przedstawił swoje stanowisko:

1. Zarząd Spółki nie podziela stanowiska kontrolującego, co do jakości sprzętu, z uwagi na fakt, iż wskazane powyżej 26,5 % sprzętu jest nieużytkowane i zostało zgromadzone w serwerowni w celu likwidacji. Jednocześnie informujemy, że w bieżącym roku zostały zakupione: 4 stacje robocze wraz z monitorami do działu TE, 1 komputer do działu GF, 1 komputer do Kadr oraz 2 laptopy do działu TE i TEG spełniające potrzeby pracowników i systemu informatycznego Spółki.
2. Zgodnie z sugestią zawartą w punkcie 3 b) i 3 c), Zarząd Spółki zaplanuje w planach rzeczowo-finansowych na rok 2015 nabycie programu Axence nVision lub uplook (wartość programu ok. 10 000,00 zł), co pozwoli na kontrolę dostępu do dysku C i D, uniemożliwi swobodne ściąganie i instalowanie oprogramowania przez użytkownika do tego nieuprawnionego oraz zgrywania na wszelkiego rodzaju nośniki materiałów do których prawo przetwarzania i archiwizowania ma Spółka.

ZALECENIA POKONTROLNE:

1. Zaleca się w trybie pilnym dokonanie przez Dział NI „inventaryzacji jakościowej” komputerów i przekazanie Zarządowi Spółki raportu w zakresie konieczności zakupu sprzętu bardzo dobrego (ilość, jakość, ceny).

Bieżące procesy informatyczne wymagają zabezpieczenia w dostateczną ilość nośników informacji (m.in. pendriv'y, papier do drukarek). Należy racjonalnie gospodarować nośnikami (ewidencja zużycia) pod nadzorem Działu NI.


2. Zaleca się wprowadzenie blokad dostępu do stron internetowych nie związanych z wypełnianiem obowiązków służbowych, a mogących być wykorzystywanymi przez pracowników Spółki w celach prywatnych np. portale społecznościowe np. Facebook czy internetowe zakupy/aukcje np. Allegro. Przyjęcie założenia, iż zdarzenia tego typu są incydentalne nie jest wystarczającym argumentem dla zabezpieczenia Spółki przed nieuzasadnionymi kosztami oraz łamaniem regulaminowych zasad pracy przez pracowników.

3. Zaleca się kontynuowanie prac zmierzających do zabezpieczenia sprzętu komputerowego Spółki i uniemożliwienia zgrywania na wszelkiego rodzaju nośniki materiałów do których prawo przetwarzania i archiwizowania ma Spółka oraz uniemożliwienie kopiowania oprogramowania, do którego Spółka posiada licencje lub jest jego właścicielem.

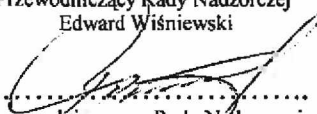
4. Zaleca się podjęcie próby zablokowania z poziomu użytkownika dostępu do dysku C i/lub D, możliwości instalacji na stacji roboczej niepowołanego oprogramowania oraz ściągania z sieci danych (w tym zdjęcia, muzyka, filmy). Stwierdzenie takich faktów przez instytucje kontroli zewnętrznej może doprowadzić do poniesienia przez Zarząd odpowiedzialności prawnej a Spółkę na straty finansowe z tytułu użytkowania „pirackich” programów lub archiwizowania treści multimedialnych bez posiadania do nich praw.

5. Respektować harmonogram prac wdrożeniowych od firmy UNISOFT.

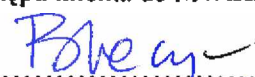
6. Doprowadzić do skutecznego wdrożenia komputerowego systemu dostępu klienta do MWiK.



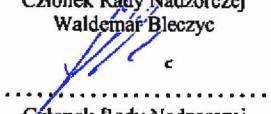
 Przewodniczący Rady Nadzorczej
 Edward Wiśniewski



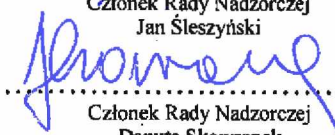
 Z-ca Przewodniczącego Rady Nadzorczej
 Bohdan Pirzecki



 Członek Rady Nadzorczej
 Waldemar Bleczyk



 Członek Rady Nadzorczej
 Jan Śleszyński



 Członek Rady Nadzorczej
 Danuta Skowronek

