



POLITYKA BEZPIECZEŃSTWA TELEINFORMATYCZNEGO W RPWIK TYCHY S.A.

Wersja:	01/2018
Data wersji:	22.11.2018 r.
Utworzony przez:	mgr inż. Łukasz Grabowski
Zatwierdzony przez:	Krzysztof Zalwowski – Prezes Zarządu
Poziom poufności:	1

Niniejsza instrukcja reguluje sposób nadawania upoważnień użytkownikom sieci, należącej do RPWiK Tychy S.A. Zawarte są w niej również prawa i obowiązki pracowników firmy, sposoby tworzenia kopii zapasowych danych. Ponadto, opisuje ona zakres odpowiedzialności w zarządzaniu siecią oraz treścią.



Spis treści

POSTANOWIENIA OGÓLNE	3
ZDARZENIA ZAGRAŻAJĄCE BEZPIECZEŃSTWU DANYCH I PRACA W TRYBIE AWARYJNYM	7
ZABEZPIECZENIE SYSTEMU INFORMATYCZNEGO PRZED ZJAWISKAMI FIZYCZNYMI	8
FIZYCZNE ZABEZPIECZENIE SYSTEMU INFORMATYCZNEGO PRZED OSOBAMI NIEUPOWAŻNIONYMI.....	9
KONTROLA DOSTĘPU DO SYSTEMÓW INFORMATYCZNYCH	11
KOMPUTEROWA SIEĆ PUBLICZNA, A SIEĆ FIRMOWA.....	15
PRZESYŁANIE DANYCH DO PODMIOTÓW ZEWNĘTRZNYCH	16
ZABEZPIECZENIE OPROGRAMOWANIA I ARCHIWIZACJA DANYCH.....	17
OCHRONA DANYCH PRZED WIRUSAMI I PROGRAMAMI SZPIEGOWSKIMI.....	22
ADMINISTRATOR SYSTEMU INFORMATYCZNEGO	22
KONTROLA WEWNĘTRZNA	23
POSTANOWIENIA KOŃCOWE.....	24

Inspektor Ochrony Danych

Łukasz Grabowski

wersja 01/2018 z 22.11.2018 r.

PREZES ZARZĄDU
Dyrektor Naczelny

mgr inż. Krzysztof Załowski

WICEPREZES ZARZĄDU
Dyrektor ds. Technicznych

mgr inż. Marek Dygoń

RPWiK Tychy S. A.
Kierownik Działu Informatyki
i Bezpieczeństwa Informacji

mgr inż. Dariusz Mrowiec



POSTANOWIENIA OGÓLNE

§ 1

1. Niniejsza polityka bezpieczeństwa teleinformatycznego normuje zagadnienia związane z bezpieczeństwem danych komputerowych gromadzonych, przetwarzanych, transmitowanych lub przechowywanych w Rejonowym Przedsiębiorstwie Wodociągów i Kanalizacji w Tychach Spółka Akcyjna (dalej „RPWiK Tychy S.A.”). W szczególności określa ona sposób zabezpieczenia systemów komputerowych przed dostępem do nich osób nieupoważnionych, tryb tworzenia kopii bezpieczeństwa i archiwizacji danych.
2. Zaleca się regularne przeprowadzanie audytów systemu bezpieczeństwa informatycznego. Audyty te powinny obejmować zadania takie jak testy penetracyjne, testy kontrolne - należy do nich również analiza systemowa, wykonana jedną ze znanych technik. Ma ona na celu teoretyczną ocenę bezpieczeństwa systemu informatycznego.

§ 2

Przez użyte w Instrukcji określenia należy rozumieć:

1. Administrator Systemu Informatycznego (ASI) - osoba nadzorująca pracę systemu informatycznego oraz wykonującą w nim czynności wymagające specjalnych uprawnień;
2. autoryzacja – nadanie uprawnienia na dostęp do konkretnych informacji lub zasobów;
3. baza danych - zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze rekordów lub obiektów, w których są zapisane dane jednostkowych obiektów;
4. bomba logiczna - nazwa kodu zawartego w legalnym programie, mającego się aktywnić w określonych warunkach np. pojawienie się konkretnego



użytkownika, obecność pewnego pliku na dysku lub data oraz wpływającego destrukcyjnie na działanie systemu informatycznego;

5. certyfikat klucza – sekwencja danych opatrzona przez Ośrodek Certyfikacji podpisami cyfrowymi, która zawiera co najmniej: nazwę Ośrodka Certyfikacji, identyfikator użytkownika, klucz publiczny użytkownika, określenie okresu ważności oraz numer seryjny;
6. firewall – urządzenie, program, którego głównym zadaniem jest zabezpieczenie sieci wewnętrznej przed nieuprawnionym dostępem z zewnątrz, jak również zapewnienie kontrolowanego dostępu użytkowników wewnętrznych w przypadku rozbudowanych sieci wewnętrz danej organizacji;
7. hasło - słowo złożone z liter, cyfr lub innych znaków, które musi podać użytkownik, aby mógł korzystać z dostępu do zastrzeżonych zasobów np. sieci komputerowej, bazy danych, komputera. Hasło jest jednym ze sposobów ochrony danych przed osobami nieupoważnionymi;
8. jednostki organizacyjne – komórki organizacyjne firmy;
9. Kierownik – Kierownik, Dyrektor albo inna osoba pełniąca funkcje kierownicze;
10. klucz publiczny – parametr przekształcenia matematycznego, który może zostać podany do publicznej wiadomości używany do weryfikacji podpisów cyfrowych utworzonych z użyciem odpowiadającego mu klucza prywatnego. Klucze publiczne są również używane do szyfrowania wiadomości lub plików które mogą zostać później odszyfrowane z udziałem odpowiadających im kluczy prywatnych;
11. koń trojański – program, który udaje pracę innego legalnego programu, a w międzyczasie wykonuje szereg niepożądanych czynności (np. fałszywy program „login” kradnie hasło użytkownika);
12. kopie archiwalne – kopie plików danych lub plików oprogramowania tworzone na nośniku wymiennym lub dysku twardym komputera, przeznaczone do ich trwałego przechowywania, jak również do odtworzenia danych w przypadku ich utraty lub uszkodzenia;



13. kopie bezpieczeństwa – kopie plików danych lub plików programowania tworzone na nośniku wymiennym lub dysku twardym komputera w celu ich odtworzenia w przypadku utraty lub uszkodzenia danych;
14. nośnik komputerowy (wymienny) – nośnik służący do zapisu informacji, np. karta pamięci, płyta CD, wymienny dysk twardy, pendrive;
15. plik - ciąg bajtów posiadający swoją nazwę oraz parametry odróżniające go od innych plików: rozmiar, datę powstania lub datę ostatniej modyfikacji itp.;
16. pliki logów - pliki - dzienniki zawierające informacje o czasie i rodzajach zdarzeń występujących w systemie informatycznym;
17. Polityka Bezpieczeństwa Informacji – zespół procedur dotyczących ochrony informacji w Rejonowym Przedsiębiorstwie Wodociągów i Kanalizacji w Tychach Spółka Akcyjna;
18. program komputerowy – zbiór instrukcji, które po umieszczeniu na rozpoznawalnym przez urządzenie nośniku i automatycznym przetłumaczeniu na język zrozumiały dla tego urządzenia powoduje, że osiąga on zdolność do wykonywania danej czynności lub też wykonuje daną czynność;
19. serwer - wyróżniony specjalistyczny komputer świadczący usługi na rzecz mających z nim łączność innych komputerów, np. przechowujący pliki, pośredniczący w przekazywaniu poczty itp.;
20. sieć komputerowa - połączenie komputerów umożliwiające im dzielenie się swoimi zasobami takimi jak: pamięć dyskowa, programy, urządzenia peryferyjne;
21. sieć publiczna – sieć komputerowa, np. Internet;
22. pracownik IT - pracownicy odpowiedzialni za należytne funkcjonowanie systemów informatycznych;
23. system autentyfikacji użytkownika – proces weryfikacji dostępu użytkownika do systemu informatycznego opierający się na identyfikatorach lub hasłach;



24. system informatyczny (system) – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
25. teletransmisja danych - przesyłanie danych przy pomocy dostępnych łączy;
26. Firma – Rejonowe Przedsiębiorstwo Wodociągów i Kanalizacji w Tychach Spółka Akcyjna.
27. firmowa sieć komputerowa – własna lub dzierżawiona sieć komputerowa wraz z wszelkimi zasobami teleinformatycznymi będącymi własnością Rejonowego Przedsiębiorstwa Wodociągów i Kanalizacji w Tychach Spółka Akcyjna;
28. urządzenie mechaniczne uniemożliwiające swobodne przenoszenie sprzętu – urządzenie uniemożliwiające przenoszenie sprzętu poza obszar pomieszczenia służbowego użytkownika bez zgody dysponenta bądź pokonania zastosowanych zabezpieczeń mechanicznych;
29. uwierzytelnianie – proces potwierdzenia tożsamości osoby, urządzenia lub integracji danych;
30. użytkownik – pracownik posiadający uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych, użytkownik z uprawnieniami na poziomie Administratora staje się Administratorem systemu;
31. ważne dane - dane wymagające szczególnej ochrony ze względu na interes Firmy oraz objęte tajemnicą ze względu na dobro wizerunkowe Rejonowego Przedsiębiorstwa Wodociągów i Kanalizacji w Tychach Spółka Akcyjna;
32. wirus - program, który uaktywniony w pamięci operacyjnej, powoduje wadliwe działanie, zniszczenie lub modyfikację systemu operacyjnego, programu komputerowego lub danych;

§ 3

1. Za stan bezpieczeństwa danych komputerowych, zainstalowanego oprogramowania oraz sprzętu komputerowego odpowiedzialne są władze Firmy



oraz Kierownicy danych działów. Za zabezpieczenie danych komputerowych, oprogramowania i sprzętu komputerowego poszczególnych stanowisk odpowiedzialni są ich użytkownicy.

2. Wszyscy użytkownicy systemu informatycznego zobowiązani są do zapoznania się z przepisami normującymi kwestie związane z bezpieczeństwem systemów teleinformatycznych w Firmie oraz złożenia u bezpośredniego przełożonego stosownego oświadczenia.

ZDARZENIA ZAGRAŻAJĄCE BEZPIECZEŃSTWU DANYCH I PRACA W TRYBIE AWARYJNYM

§ 4

1. Do zdarzeń zagrażających bezpieczeństwu danych należą:
 - a. próby naruszenia ochrony danych:
 - z zewnątrz: włamania do systemu, podsłuch, kradzież danych,
 - z wewnętrz: nieumyślna lub celowa modyfikacja danych, ich kradzież lub zniszczenie;
 - b. programy destrukcyjne tj. wirusy, konie trojańskie, bomby logiczne;
 - c. awarie sprzętu lub uszkodzenie oprogramowania;
 - d. kradzież sprzętu lub nośników z ważnymi danymi;
 - e. inne, skutkujące utratą danych np. klęski żywiołowe.
2. W przypadku stwierdzenia naruszenia ochrony danych, w szczególności zaistnienia zdarzenia mogącego wpłynąć negatywnie na organizację, pracownik Firmy zobowiązany jest natychmiast powiadomić o zaistniałym zdarzeniu bezpośredniego przełożonego, Administratora danego systemu oraz Inspektora Ochrony Danych (IOD).
3. Inspektor Ochrony Danych, we współpracy z odpowiednimi pracownikami Firmy, podejmuje działania w celu:



- a. określenia miejsca, sytuacji i czasu, w jakim stwierdzono naruszenie bezpieczeństwa;
 - b. określenia symptomów naruszenia bezpieczeństwa;
 - c. określenia wszelkich informacji mogących wskazać na przyczynę naruszenia;
 - d. oszacowania strat w systemie;
 - e. naprawy uszkodzeń, w szczególności odtworzenia danych.
4. W celu odtworzenia danych należy wykorzystywać kopie bezpieczeństwa oraz archiwalne, których procedury tworzenia zawarte zostały w § 26-29.
 5. Każde zdarzenie zagrażające bezpieczeństwu danych lub każde zdarzenie, które spowodowało naruszenie ochrony danych, winno zostać pisemnie udokumentowane przez Inspektora Ochrony Danych, poprzez sporządzenie przez niego stosownej notatki oraz zgłoszenie zaistniałej sytuacji do odpowiedniego organu nadzorczego. Procedura ta opisana jest w pozostałych załącznikach do Polityki Bezpieczeństwa Informacji.

ZABEZPIECZENIE SYSTEMU INFORMATYCZNEGO PRZED ZJAWISKAMI FIZYCZNYMI

§ 5

1. Pomieszczenia, w których eksploatowane są urządzenia komputerowe oraz pomieszczenia, w których przechowywane są nośniki danych, powinny być:
 - a. wolne od zagrożeń związanych ze zjawiskami fizycznymi typu:
 - wyładowania elektrostatyczne i atmosferyczne (np. elektryzujące się wykładziny, sąsiedztwo urządzeń odgromowych),
 - silne działanie pól elektromagnetycznych (np. bliskie sąsiedztwo stacji transformatorowych i urządzeń rozdzielczych wysokiego napięcia, pól magnetycznych pochodzących od urządzeń z silnikami elektrycznymi wysokiej mocy lub od transformatorów zasilania budynków itp.);



- b. zabezpieczone systemem ochrony p.poż.;
- c. zabezpieczone przed zalaniem.
2. Serwerownia ma zapewnione stałe utrzymywanie temperatury, wilgotności i innych parametrów określonych przez producenta sprzętu komputerowego. Zabezpieczenie przed zanikiem prądu jest zapewnione poprzez zastosowanie awaryjnych zasilaczy bezprzerwowych (UPS) i/lub agregatów prądotwórczych.
3. Polecanym rozwiązaniem jest korzystanie z usług chmurowych. Ważne jest należyte sprawdzenie referencji, jakimi może pochwalić się usługodawca. Do usług chmurowych można przenieść np. kopie zapasowe danych (Oracle, Xopero, Microsoft). Serwerem chmurowym można zastąpić jego fizyczny odpowiednik (Oktawave, Kylos i inne).
4. Szafy, w których przechowywane są nośniki magnetyczne, powinny zapewniać ochronę przed czynnikami zewnętrznymi, mogącymi doprowadzić do utraty danych.

FIZYCZNE ZABEZPIECZENIE SYSTEMU INFORMATYCZNEGO PRZED OSOBAMI NIEUPOWAŻNIONYMI

§ 6

1. Serwery, profesjonalne stacje robocze, urządzenia teletransmisyjne, szafy teletechniczne, wyłączniki zasilania elektrycznego, szafy z nośnikami magnetycznymi zawierające kopie danych, powinny być usytuowane w pomieszczeniu uniemożliwiającym dostęp do nich osób nieupoważnionych.
2. Dostęp do pomieszczeń, o których mowa, winien być ścisłe kontrolowany poprzez zainstalowane systemy alarmowe oraz kontrolę dostępu do pomieszczeń.
3. Zaleca się dodatkowe zabezpieczenie serwerów oraz komputerów, w których zapisane są ważne dane, poprzez zastosowanie urządzeń mechanicznych uniemożliwiających swobodne przemieszczanie oraz utrudniających ich ewentualną kradzież.



§ 7

1. Lokalizacja urządzeń komputerowych (komputerów typu PC, terminali, drukarek) w pomieszczeniach użytkowanych przez pracowników powinna uniemożliwiać osobom postronnym dostęp do nich, a także wgląd do danych wyświetlanych na monitorach komputerowych.
2. W przypadku oddalenia się pracownika od stanowiska pracy, należy pozostawić system w stanie blokady (zablokować komputer), aby osoby nieupoważnione nie miały do niego dostępu. W takich przypadkach stosujemy wygaszacz ekranu o krótkim czasie aktywacji, wraz z zabezpieczeniem w postaci mocnego hasła. Należy pamiętać o zasadzie czystego biurka.

§ 8

1. Wszelkie prace konserwacyjne i naprawcze urządzeń komputerowych oraz uaktualnienia systemu informatycznego, wykonywane przez firmę zewnętrzną, powinny odbywać się na zasadach określonych w szczegółowej umowie pomiędzy Firmą, a tymże podmiotem, z uwzględnieniem klauzuli dotyczącej ochrony przez Zleceniodobiorcę wszelkich informacji, do których ma dostęp w czasie wykonywania usługi. Firma zewnętrzna powinna być dostosowana do przepisów RODO.
2. Prace, o których mowa w pkt. 1. powinny zostać odnotowane w rejestrze wykonanych usług/napraw prowadzonym przez tenże podmiot.
3. W przypadku naprawy sprzętu komputerowego w serwisie zewnętrznym, ważne dane należy zabezpieczyć (zarchiwizować) oraz o ile jest to możliwe, usunąć z nośników informacji.
4. Po modyfikacjach wykonywanych przez firmę zewnętrzną, zaleca się niezwłoczną zmianę haseł.



§ 9

1. Wszyscy użytkownicy z jednostek administracyjnych Firmy zobowiązani są do przekazywania uszkodzonych nośników komputerowych, zawierających ważne dane, do odpowiedniej osoby (ASI).
2. Przekazanie powinno zostać potwierdzone protokołem przekazania i odbioru.
3. Uszkodzone nośniki komputerowe, zawierające ważne dane, powinny być fizycznie niszczone przy udziale wyspecjalizowanej firmy, która posiada odpowiednie kompetencje i pozwolenia. Z wykonanych czynności firma świadcząca ww. usługi powinna sporządzić protokół.
4. Do czasu zniszczenia, nośniki komputerowe powinny być zabezpieczone przed dostępem osób nieupoważnionych.

§ 10

1. Za bezpieczeństwo komputerów przenośnych odpowiedzialni są ich użytkownicy.
2. Komputery, o których mowa w pkt. 1., po zakończonej pracy, powinny być przechowywane w warunkach zapewniających ich bezpieczeństwo. Dopuszcza się zabezpieczenie ich poprzez użycie urządzeń mechanicznych uniemożliwiających swobodne przemieszczanie sprzętu oraz utrudniających ewentualną kradzież.
3. Wynoszenie komputera przenośnego poza siedzibę firmy, bez odpowiedniego zezwolenia, jest niedozwolone.

KONTROLA DOSTĘPU DO SYSTEMÓW INFORMATYCZNYCH

§ 11

1. Dostęp do systemu informatycznego mogą posiadać:
 - a. pracownicy – w zależności od wykonywanych czynności służbowych;



- b. wykonawcy usług oraz dostawcy sprzętu lub oprogramowania – w zakresie koniecznym do realizowania danej usługi lub wykonania określonych czynności w systemie (za zgodą ASI);
 - c. inni użytkownicy – w zakresie ustalonym w stosowniej umowie.
2. Osoby, o których mowa powyżej, mogą posiadać w systemie własne konto, do którego dostęp winien być możliwy jedynie po podaniu właściwego identyfikatora i hasła.
 3. Właściciel konta odpowiedzialny jest za wszelkie działania wykonane z użyciem jego identyfikatora.
 4. Pracownicy dostawców sprzętu i oprogramowania wykonują usługę tylko za zgodą ASI i IOD. Jeśli rodzaj wykonywanych czynności (np. aktualnienie, poprawienie błędnej lub wadliwie działającej konfiguracji oprogramowania czy sprzętu) wymusza pracę na kontach administracyjnych – usługa winna być nadzorowana przez ASI i IOD.

§ 12

1. Zabronione jest:
 - a. udostępnianie identyfikatorów i haseł osobom postronnym;
 - b. łamanie haseł;
 - c. dokonywanie włamań na konta innych użytkowników;
 - d. nieprawne uzyskiwanie dostępu do kont administracyjnych;
 - e. zakłócanie działania usług;
 - f. omijanie zabezpieczeń (nie dotyczy audytu lub testowania);
 - g. rozprowadzanie wirusów, robaków i koni trojańskich oraz niechcianej poczty (spam);
 - h. praca na koncie innego użytkownika, za wyjątkiem sytuacji, w których wymagają tego prace konserwacyjne;
 - i. podejmowanie innych działań, mogących być zagrożeniem dla systemu.



2. Wykonywanie zabronionych czynności, o których mowa powyżej, stanowi ciężkie naruszenie obowiązków pracowniczych i może skutkować odpowiedzialnością karną i cywilną.
3. Zabronione jest użytkowanie sprzętu komputerowego przez osoby nie posiadające uprawnień do pracy w systemie informatycznym.
4. Wykorzystywanie służbowego sprzętu komputerowego i oprogramowania do celów prywatnych, jest niedozwolone.

§ 13

Rejestracja użytkowników w systemie informatycznym, nadawanie lub modyfikacja uprawnień oraz wyrejestrowywanie użytkowników z systemu odbywa się, zgodnie z procedurą zisaną w załączniku 8 do Polityki Bezpieczeństwa Informacji.

§ 14

1. Wszystkie systemy informatyczne muszą mieć uaktywnione posiadane mechanizmy kontroli dostępu.
2. Każdy użytkownik systemu informatycznego musi posiadać jawnego identyfikatora i wprowadzone przez siebie poufne hasło (hasła) autoryzujące jego osobę.
3. Komputery stacjonarne i przenośne powinny mieć uaktywnione posiadane mechanizmy kontroli dostępu do zasobów komputera.
4. Hasłami powinny być również zabezpieczone udostępniane wewnętrznej sieci Firmy zasoby zawierające ważne dane.
5. W celach bezpieczeństwa zaleca się:
 - a. wprowadzenie haseł na pliki zawierające ważne dane, szyfrowanie danych za pomocą kluczy publicznych i prywatnych;
 - b. uaktywnienie wygaszaczek ekranów oraz wprowadzenie haseł na nich.



§ 15

1. Hasła, o których mowa w § 14 ust. 2, 3 i 4, oraz hasła służące do administrowania systemami i programami nie są krótsze niż 8 znaków. Zaleca się stosowanie dużych i małych liter, cyfr oraz innych znaków specjalnych, co znacznie utrudni złamanie haseł np. metodą słownikową lub *brute force*.
2. O długości haseł, o których mowa w § 14 ust. 5, decyduje użytkownik.
3. Zabronione jest zapisywanie haseł w sposób jawnym oraz przekazywanie ich innym osobom lub umieszczanie w miejscu łatwo widocznym i dostępnym.
4. W przypadku prac serwisowych, zleconych przez Firmę, serwisant upoważniony jest do zresetowania hasła.

§ 16

1. Hasła służące do administrowania systemami i programami powinny być spisane oraz umieszczone w zamkniętych kopertach, oddzielnych dla każdego systemu lub programu, w miejscu uniemożliwiającym dostęp do nich osób nieupoważnionych, chroniącym przed utratą lub zniszczeniem oraz gwarantującym ich odczytanie upoważnionemu użytkownikowi, a także kierownikowi właściwej jednostki organizacyjnej Firmy, w przypadkach nadzwyczajnych. Dobrym miejscem będzie sejf.
2. Zarejestrowane hasła, o których mowa powyżej, powinny posiadać adnotację o dacie ich wprowadzenia. Kolejnym krokiem jest ich przechowywanie przez czas odpowiedni do sprawnego działania systemu.
3. Hasła, o których mowa w § 14 ust. 3, powinny zostać zabezpieczone zgodnie z procedurą określoną w ust. 1.



§ 17

1. Hasła, o których mowa w § 14 ust. 2, należy zmieniać raz na 90 dni, niezwłocznie w przypadku stwierdzenia ich ujawnienia lub podejrzenia o ujawnienie osobie nieuprawnionej.
2. Hasła służące do administrowania systemami i programami powinny być zmieniane co najmniej raz na miesiąc, niezwłocznie w przypadku stwierdzenia ich ujawnienia lub podejrzenia o ujawnienie osobie nieuprawnionej.
3. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, o których mowa w ust. 2.
4. Hasła, o których mowa w § 14 ust. 3, powinny być zmieniane co najmniej raz na 90 dni, jak również w przypadku stwierdzenia ich ujawnienia lub podejrzenia o ujawnienie osobie nieuprawnionej.
5. Hasła, o których mowa w § 14 ust. 4 i 5, powinny być zmieniane w przypadku stwierdzenia ich ujawnienia lub podejrzenia o ujawnienie osobie nieuprawnionej.
6. Hasła zachowują swoją poufność również po ustaniu ich czasu trwania.

KOMPUTEROWA SIEĆ PUBLICZNA, A SIEĆ FIRMOWA

§ 18

1. Komputerowa sieć Firmowa powinna być odseparowana od sieci publicznej za pomocą systemów typu firewall.
2. Korzystanie z usług poprzez sieć publiczną powinno mieć miejsce, po zastosowaniu przez właściwą jednostkę organizacyjną, koniecznych systemów zabezpieczeń w szczególności firewall-i oraz systemów autentyfikacji użytkownika i szyfrowania danych - VPN.

§ 19

1. Zabrania się wykonywania połączeń z systemów (serwerów, stacji zarządzających, komputerów) funkcjonujących w wewnętrznej sieci administracyjnej, do



publicznej sieci Internet, z wyjątkiem połączeń rezerwowych (awaryjnych) na wydzielonych i zabezpieczonych stanowiskach.

2. Zdalny dostęp do serwerów, w celach administracyjnych, powinien być realizowany z użyciem narzędzi zapewniających bezpieczną komunikację – szyfrowania danych i certyfikatów.

§ 20

1. Dopuszcza się obieg dokumentów elektronicznych pomiędzy jednostkami organizacyjnymi Firmy.
2. Do przesyłania dokumentów elektronicznych pomiędzy jednostkami organizacyjnymi Firmy należy stosować pocztę elektroniczną lub inne lokalne rozwiązania technologiczne.
3. Ważne dane powinny być przesyłane w formie niejawnej i umożliwiającej ich uwierzytelnienie.

§ 21

Za techniczne umożliwienie użytkownikom korzystania z zasobów internetowych, o których mowa w ust. 1, odpowiedzialna jest ASI, związany z RPWiK Tychy S.A. stosowną umową.

PRZESYŁANIE DANYCH DO PODMIOTÓW ZEWNĘTRZNYCH

§ 22

1. Do przesyłania ważnych danych do podmiotów zewnętrznych mogą być użyte systemy informatyczne, które uzyskały pozytywną opinię IOD oraz zostały przetestowane zgodnie z procedurami.
2. Systemy informatyczne służące do przesłania danych oraz generowania plików przeznaczonych do wysłania, do podmiotów zewnętrznych powinny posiadać uaktywnione mechanizmy kontroli dostępu.



3. Ważne dane należy przesyłać w formie niejawniej i umożliwiającej ich uwierzytelnienie.
4. Za przesyłanie danych, określonych w ust. 3, odpowiedzialny jest pracownik wyznaczony przez kierownika danej jednostki organizacyjnej Firmy.
5. Każde wysłanie danych winno zostać potwierdzone w systemie lub też pisemnie przez upoważnioną osobę na wydruku przesłanych danych.

§ 23

Kwestie związane z wykorzystywaniem systemów informatycznych Firmy do przekazywania danych do podmiotów zewnętrznych podlegają szczegółowym uregulowaniom w zawieranych obustronnie umowach, których procedury i klauzule dotyczące bezpieczeństwa systemów informatycznych powinny być zgodne z uregulowaniami niniejszej Polityki.

ZABEZPIECZENIE OPROGRAMOWANIA I ARCHIWIZACJA DANYCH

§ 24

1. Oprogramowanie stosowane w Przedsiębiorstwie musi pochodzić wyłącznie ze źródeł legalnych, posiadać łatwo dostępną informację o identyfikatorze wersji i numerze licencji.
2. Wykorzystywane w Firmie oprogramowanie ewidencjonowane jest w formie rejestru oprogramowania w systemie elektronicznym Administratora. Wykaz poszczególnych licencji powinien znajdować się u Kierownika/Dyrektora odpowiedniej jednostki Firmy.
3. Zabronione jest instalowanie oprogramowania nielegalnego oraz niezwiązanego merytorycznie z wykonywaną pracą, a w szczególności oprogramowania, którego eksploatacja jest sprzeczna z Ustawą o prawach autorskich i prawach pokrewnych.



4. Instalacja oprogramowania, o którym mowa w ust. 2, stanowi ciężkie naruszenie obowiązków pracowniczych, jest obłożona odpowiedzialnością karną i cywilną.
5. Dopuszcza się, po uzyskaniu zgody Kierownika/Dyrektora danego działu Firmy, instalowanie:
 - a. w celach służbowych oprogramowania darmowego (freeware-owego);
 - b. w celach służbowych - testowych oprogramowania tzw. shareware-owego, na wydzielonym stanowisku komputerowym ze wszystkimi obostrzeniami umowy licencyjnej oprogramowania.

§ 25

1. Umowy dotyczące świadczenia usług teleinformatycznych, zakupu lub modernizacji urządzeń komputerowych, systemów informatycznych i oprogramowania powinny zawierać niezbędne wymagania dotyczące bezpieczeństwa informacji lub odniesienia do odpowiednich dokumentów regulujących te kwestie w Firmie oraz zakresy odpowiedzialności stron umowy w tym względzie.
2. W celu ograniczenia ryzyka niewydolności funkcjonalnej systemów informatycznych należy prognozować przyszłe wymagania dotyczące pojemności zasobów dyskowych, mocy obliczeniowej procesorów, przepustowości sieci itd. Wymagania te powinny być określone i udokumentowane przed zaakceptowaniem i wdrożeniem nowych, i modernizowanych systemów.
3. Przed dokonaniem odbioru nowych lub modernizowanych systemów informatycznych istotnych z punktu widzenia działalności Firmy, należy ustalić kryteria ich odbioru oraz przeprowadzić testy sprawdzające.
4. Kryteria odbioru systemu informatycznego powinny uwzględniać następujące elementy:
 - a. wymagania dotyczące wydajności i pojemności;
 - b. wymagania dotyczące wdrożonych zabezpieczeń;



- c. przestrzegania procedur zarządzania incydentami zagrażającymi bezpieczeństwu informacji przetwarzanej i gromadzonej w systemie;
 - d. szkolenie w obsłudze i użytkowaniu;
 - e. optymalne warunki gwarancji i serwisu;
 - f. potwierdzenie, że instalacja nowego systemu nie będzie wpływać niekorzystnie na aktualne systemy.
5. Testowanie oprogramowania z punktu widzenia ciągłości działania Firmy, należy przeprowadzać w wydzielonym środowisku testowym.
 6. Testowanie przeprowadzają: pracownicy firmy IT wybranej przez RPWiK Tychy S.A. oraz osoby merytorycznie odpowiedzialne za funkcjonowanie systemu, wyznaczone przez RPWiK Tychy S.A. (ASI).
 7. Zmiany w istotnych, z punktu widzenia funkcjonowania Firmy, programach podlegają takim samym rygorom, jak włączenie do eksploatacji nowego oprogramowania.

§ 26

1. Bazy danych, oprogramowanie oraz konfiguracja systemów operacyjnych w jednostkach Firmy powinny być zabezpieczone w postaci kopii bezpieczeństwa lub danych archiwalnych oraz posiadać oryginalne nośniki instalacyjne.
2. Należy wykonywać następujące kopie bezpieczeństwa:
 - a. przed dokonaniem zmian w konfiguracji systemów operacyjnych lub oprogramowania;
 - b. przed dokonaniem zmian w programach (np. zmiana wersji);
 - c. po każdej istotnej zmianie danych w bazie danych.
3. Oprócz kopii, o których mowa w ust. 2, należy wykonywać kopie archiwalne:
 - a. miesięczne – na koniec danego miesiąca;
 - b. roczne – na koniec danego roku.



-
4. Za wykonanie i zabezpieczenie kopii, określonych w ust. 2 i 3, odpowiedzialny jest Administrator danego systemu (firma zewnętrzna) lub Administrator Systemu Informatycznego RPWiK Tychy S.A., który fakt sporządzenia kopii odnotowuje w odpowiednim dzienniku.

§ 27

Kopie bezpieczeństwa i archiwalne należy:

1. wykonać w co najmniej dwóch egzemplarzach każda, przy czym przynajmniej jedną na nośniku wymiennym;
2. przechowywać w dwóch różnych urządzeniach i miejscach, innych niż te, w których eksploatowane zbiory przechowywane są na bieżąco, zaleca się wykonywanie kopii w usługach chmurowych.

§ 28

1. Kopie bezpieczeństwa należy przechowywać do momentu wykonania następnej kopii bezpieczeństwa.
2. Kopie archiwalne miesięczne należy przechowywać przez okres 1 roku, a kopie roczne przez okres 5 lat.

§ 29

Nośniki komputerowe, na których znajdują się kopie bezpieczeństwa i dane archiwalne, powinny być oznaczone w sposób trwały, jednoznaczny i czytelny i zaewidencjonowane w odpowiednim rejestrze.

§ 30

1. Kopie archiwalne należy:
 - a. okresowo sprawdzać pod kątem ich dalszej przydatności do odtwarzania;
 - b. bezzwłocznie usuwać po ustaniu ich użyteczności.



2. Usuwanie kopii danych następuje poprzez bezpieczne kasowanie. Nośniki tych danych, na których zapisywane są kopie bezpieczeństwa niszczy się na trwale w sposób mechaniczny.

§ 31

1. W oddziałach Firmy ważne dane przychodzące pocztą elektroniczną powinny być zabezpieczone w nośniku wymiennym lub lokalnym dysku twardym komputera.
2. O trybie archiwizowania danych decyduje Administrator Systemu Informatycznego odpowiedzialny za obsługę poczty elektronicznej.
3. Okres przechowywania kopii, określonych w ust. 1, powinien wynikać z rodzaju zarchiwizowanych danych oraz być zgodny z przepisami Firmy.

§ 32

1. W celach bezpieczeństwa należy archiwizować istotne dane zapisane na dyskach twardych komputerów poszczególnych użytkowników, w szczególności dane z komputerów przenośnych.
2. O trybie archiwizowania danych, o których mowa w ust. 1, decyduje użytkownik. Przekazanie do pracy komputera używanego powinno nastąpić po usunięciu zbędnych danych i oprogramowania przez służby informatyczne w porozumieniu z poprzednim użytkownikiem.
3. Oprogramowanie oraz bazy danych, które przestały być wykorzystywane w Firmie, należy usunąć z urządzeń komputerowych po dokonaniu ich uprzedniej archiwizacji.



OCHRONA DANYCH PRZED WIRUSAMI I PROGRAMAMI SZPIEGOWSKIMI

§ 33

1. Potencjalnymi źródłami przedostawania się programów szpiegowskich oraz wirusów komputerowych na urządzenia komputerowe używane w Firmie są:
 - a. załączniki do poczty elektronicznej;
 - b. przeglądane strony internetowe;
 - c. pliki i aplikacje pochodzące z nośników wymiennych, uruchamiane i odczytywane na stacji roboczej.
3. W celu zapewnienia ochrony antywirusowej, Administrator Systemu Informatycznego lub użytkownik, jest odpowiedzialny za zarządzanie systemem wykrywającym i usuwającym wirusy. System antywirusowy powinien być skonfigurowany w następujący sposób:
 - a. rezydentny monitor antywirusowy (uruchomiony w pamięci operacyjnej) powinien być stale włączony;
 - b. antywirusowy skaner ruchu internetowego powinien być stale włączony;
 - c. monitor zapewniający ochronę przed wirusami makr w dokumentach MS Office powinien być stale włączony;
 - d. skaner poczty elektronicznej powinien być stale włączony.

ADMINISTRATOR SYSTEMU INFORMATYCZNEGO

§ 34

1. Administratora Systemu Informatycznego wybiera i upoważnia Zarząd RPWiK Tychy S.A.
2. W Firmie prowadzone są rejesty Administratorów.
3. Rejestr, o którym mowa w ust. 2 winien zawierać:
 - a. imię i nazwisko Administratora;



- b. nazwę systemu informatycznego, którym administruje osoba określona w pkt. a.;
 - c. nr. telefonu Administratora, adres email.;
 - d. daty wpisania i wykreszenia z rejestru.
5. ASI może zostać osoba posiadająca odpowiednie kwalifikacje, potwierdzone ukończonymi szkoleniami lub doświadczeniem zawodowym.
 6. Podstawowym obowiązkiem Administratora Systemu jest:
 - a. zapewnienie ciągłości pracy systemu;
 - b. zarządzanie pracą systemu informatycznego, jego zasobami i użytkownikami;
 - c. czuwanie nad bezpieczeństwem zasobów systemu;
 - d. konsultacje i zgłoszenie uwag o zauważonych anomaliiach.
 7. Administrator Systemu Informatycznego powinien być dostępny dla użytkowników w godzinach swojej pracy.

KONTROLA WEWNĘTRZNA

§ 35

1. Do kontroli stanu bezpieczeństwa systemu informatycznego w komórkach organizacyjnych Firmy upoważnieni są:
 - a. Zarząd RPWiK Tychy S.A.,
 - b. IOD,
 - c. upoważnieni przez Zarząd Firmy pracownicy kontroli wewnętrznej.
2. Raz w roku IOD przedstawia Zarządowi sprawozdanie z wyników kontroli stanu zabezpieczenia systemów informatycznych w Firmie.



POSTANOWIENIA KOŃCOWE

§ 36

Zobowiązuje się wszystkich pracowników RPWiK Tychy S.A. do bezwzględnego przestrzegania ustaleń niniejszej instrukcji.