Tychy, 01.08.2005 r.

ZAŁĄCZNIK NR 1

POLITYKA BEZPIECZEŃSTWA

RPWiK TYCHY S. A.

1. Podstawa prawna

„Polityka bezpieczeństwa" stanowi wykonanie obowiązku, o którym mowa w §4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. *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), zwanego dalej „rozporządzeniem".

Celem bezpieczeństwa jest zapewnienie ochrony danych osobowych zgodnie z ustawą o ochronie danych osobowych z dnia 29.08.1997 r., Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. oraz PN ISO/IEC 17799 dla zbioru o nazwie ***„Zbiór danych osobowych klientów RPWiK Tychy S. A."***.

2. Zakres stosowania

Polityka bezpieczeństwa dotyczy przetwarzania danych osobowych przez RPWiK Tychy S. A. i zawiera następujące informacje:

A. wykaz pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe (obszar przetwarzania danych osobowych) oraz podział odpowiedzialności,
B. wykaz zbiorów danych osobowych i programów zastosowanych do przetwarzania danych,
C. opis struktury zbiorów, zawartości poszczególnych pól informacyjnych i powiązania pomiędzy nimi,
D. sposób przepływu danych pomiędzy poszczególnymi systemami,
E. środki techniczne i organizacyjne niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Celem przetwarzania danych w zbiorze RPWiK Tychy S. A. jest realizacja umów na dostawę wody, odbiór ścieków, usługi (usługi związane z dostarczeniem wody i ścieków np. czyszczenie kanalizacji, wynajem sprzętu np. koparek, usługi geodezyjne oraz projektowe, badanie sieci wodociągowo-kanalizacyjnej) oraz ewentualna wewnętrzna windykacja należności.

A. Obszar przetwarzania danych osobowych:

Obszarem przetwarzania danych osobowych w RPWiK Tychy S. A. są pomieszczenia znajdujące się w następujących lokalizacjach:

1.	Siedziba RPWiK Tychy S. A.	-	43-100 Tychy, ul. Sadowa 4
2.	Oddział Bieruń	-	43-150 Bieruń, ul. Pszenna 20
3.	Oddział Brzeszcze	-	32-626 Jawiszowice, ul. Wodna 39
4.	Oddział Czechowice Dziedzice	-	43-502 Czechowice Dziedzice ul. Legionów 85
5.	Oddział Łaziska Górne	-	43-170 Łaziska Górne, ul. Świerczewskiego

Szczegółowy wykaz budynków, pomieszczeń lub części pomieszczeń w odniesieniu do zbiorów danych znajduje się również w dokumencie „Obszar przetwarzania danych”, stanowiącym załącznik nr A do Polityki Bezpieczeństwa.

Budynki lub pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób dopuszczonych do danych osobowych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.

Pomieszczenia i budynki, o których mowa w pkt 2 powinny mieć następujące zabezpieczenia:

A. drzwi do pomieszczeń, w których przetwarzane są dane osobowe są zamykane na klucz,

B. wejście do pomieszczeń autoryzowane kartą dostępową zgodnie z nadanymi uprawnieniami,

C. dokumenty z danymi osobowymi powinny być zamykane na klucz w szafach lub sejfach,

D. budynek musi podlegać ochronie i monitorowaniu w systemie 24 godzinnym przez wszystkie dni w roku przez pracowników ochrony.

Podział odpowiedzialności w RPWiK Tychy S. A.

Administrator Danych	-	RPWiK Tychy S. A. Reprezentowany przez Zarząd Spółki Akcyjnej
Administrator Bezpieczeństwa Informacji	-	Dariusz Mrowiec
Administratorzy Zbiorów (Lokalny Administrator Bezpieczeństwa Informacji) :		
Administrator Zbioru (Oddział Łaziska Górne)	-	Janusz Michułka
Administrator Zbioru (Oddział Czechowice – Dziedzice)	-	Anna Morończyk
Administrator Zbioru (Oddział Bieruń)	-	Janusz Chwierut
Administrator Zbioru (Oddział Brzeszcze)	-	Anna Morończyk
Administrator Zbioru (Centrala Tychy)	-	Kierownicy wszystkich działów

Za realizację zabezpieczeń pomieszczeń odpowiedzialny jest FA - Dział Administracyjno – Gospodarczy.

B. Wykaz zbiorów danych osobowych i programów zastosowanych do przetwarzania danych.

W RPWiK Tychy S. A. przetwarzane są następujące zbiory danych:

1) w systemie informatycznym:
   - zbiór kadrowy
   - zbiór płacowy
   - zbiór pracowniczy (transport, stanowiska itp.)
   - zbiór klientów RPWiK Tychy S. A.
   - ……

2) kartoteki papierowe:
   - zbiór kadrowy
   - zbiór płacowy
   - zbiór pracowniczy (transport, stanowiska itp.)
   - zbiór klientów RPWiK Tychy S. A.
   - ……

Szczegółowy wykaz zbiorów danych przetwarzanych w systemie informatycznym w RPWiK Tychy S. A. i programów zastosowanych do przetwarzania danych stanowi załącznik nr B, do niniejszej Polityki Bezpieczeństwa pt. - „Wykaz przetwarzanych zbiorów danych".

Szczegółowy wykaz zbiorów danych przetwarzanych w sposób tradycyjny w postaci kartotek papierowych w RPWiK Tychy S. A. stanowi załącznik nr C, do niniejszej Polityki Bezpieczeństwa pt. - „Ewidencja zasobów danych osobowych RPWiK Tychy S. A.".

C. Opis struktury zbiorów, zawartości poszczególnych pól informacyjnych i powiązania pomiędzy nimi.

Pola informacyjne (rodzaje przetwarzanych danych) w odniesieniu do poszczególnych zbiorów zostały określone w dokumencie „Wykaz przetwarzanych zbiorów danych", stanowiącym załącznik nr B do Polityki bezpieczeństwa.

D. Sposób przepływu danych pomiędzy poszczególnymi systemami.

W ramach procesów przetwarzania danych sposób przepływu danych pomiędzy różnymi systemami informatycznymi został określony w dokumencie „Wykaz przetwarzanych zbiorów danych", stanowiącym załącznik nr B do Polityki bezpieczeństwa.

E. Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

1. Do elementów zabezpieczenia danych osobowych w RPWiK Tychy S. A. zalicza się:

a) stosowane metody ochrony pomieszczeń, w których przetwarzane są dane osobowe (zabezpieczenia fizyczne),

b) zabezpieczenie przetwarzania danych (w szczególności dokumentów papierowych i informatycznych),

c) nadzór Administratora Danych Osobowych oraz Administratora Bezpieczeństwa Informacji nad wprowadzonymi zasadami i procedurami zabezpieczenia danych (zabezpieczenia organizacyjne),

d) zabezpieczenie danych przez wszystkie podmioty i osoby biorące udział w przetwarzaniu danych (osoby upoważnione do przetwarzania danych osobowych),

e) zabezpieczenia programowe.

2. W RPWiK Tychy S. A. rozróżnia się następujące kategorie środków zabezpieczeń danych osobowych:

a) Zabezpieczenia fizyczne

- Pomieszczenia, w których są przetwarzane oraz przechowywane dane osobowe zabezpieczono poprzez system czytników kart wejściowych identyfikujący osoby uprawnione do wejścia,
- Pomieszczenia, w których przechowywane są dane osobowe wyposażono w sejf antywłamaniowy klasy A oraz podwójne drzwi antywłamaniowe klasy C,
- Na terenie RPWiK Tychy S. A. oraz jego oddziałów dyżuruje firma ochroniarska mająca za zadanie m.in. uniemożliwiać dostęp do pomieszczeń osobom nieupoważnionym.

b) Zabezpieczenia organizacyjne, w tym organizacji pracy

- Polityka bezpieczeństwa teleinformatycznego,
- Ewidencja osób uprawnionych do przetwarzania danych osobowych,
- Dokumentacja techniczna oraz organizacyjna systemów przetwarzających dane osobowe,
- Instrukcja określająca sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
- Dostęp do informacji (danych) w zakresie wykonywanych zadań na podstawie upoważnienia do przetwarzania danych osobowych,
- Dostęp do danych zgodnie z kompetencjami pracowników danego działu.

c) Zabezpieczenia sprzętowe

Sprzęt wykorzystywany w ramach systemu informatycznego oraz telekomunikacyjnego to:

- komputery klasy PC (DTK, HP, IBM),
- serwery: IBM (5 szt.), HP (2 szt.), Compaq (1 szt.),

- switch'e (3COM, CISCO, Planet, Surecom),
- routery Allied-Telesyn,
- modemy do połączeń serwisowych US-Robotics (oprogramowanie Symantec pcAnywhere),
- sieć komputerowa oparta na systemie WINDOWS 2000 SERVER, WINDOWS 2003 SERVER oraz Novell NetWare 4.11,
- systemy operacyjne na stacjach roboczych użytkowników: Microsoft Windows XP Professional, Microsoft Windows 98 SE.

Zabezpieczenia sprzętowe:

- urządzenia filtrujące typu np. ACAR,
- urządzenia podtrzymujące napięcie stacji roboczych użytkowników np. APC, MGE, EVER, PCM, COVER,
- główny UPS COVER „RT Partner" dla systemu teleinformatycznego,
- sieci komputerowe oraz komputery użytkowników zabezpieczone oprogramowaniem antywirusowym,
- odpowiednie restrykcje dotyczące zasad haseł i dostępu (np. wymagana zmiana hasła co 14 dni) oraz odpowiednie uprawnieniami.

d) Zabezpieczenia programowe i transmisji

- stosowanie ograniczeń dostępowych do urządzeń teletransmisji poprzez identyfikator i hasło osób uprawnionych,
- wykorzystywanie poufnych protokołów typu IP Sec do komunikacji z urządzeniami przemysłowymi działającymi w sieci pakietowej GSM GPRS,
- zastosowane zabezpieczenia w celu ograniczenia dostępu użytkownika jedynie do konkretnych zasobów serwera poprzez: Active Directory (domenowy system użytkowników i haseł przekazywanych siecią komputerową za pomocą protokołu Kerberos),
- ograniczenie dostępu użytkowników do funkcji administratorskich na komputerach lokalnych,
- zakaz wykonywania poleceń systemowych (restricted Shell),

- rejestracja nieudanych logowań do systemu, stosowanie oprogramowania antywirusowego Symantec Ativirus, firewall i Proxy,
- dostęp do Internetu tylko dla wybranych, upoważnionych użytkowników.

Do przetwarzania danych wykorzystywana jest baza danych oparta na Microsoft SQL Server 2000.

Środki ochrony stosowane w ramach narzędzi baz danych:

- ograniczenia dostępu poprzez identyfikatory i hasła,
- dostęp do Internetu tylko dla wybranych, upoważnionych użytkowników.
- rejestracja operacji na rekordach,
- szyfrowanie bazy danych,
- archiwizacja danych.

Środki ochrony stosowane w ramach systemu użytkowego na stanowiskach użytkowych:

- ograniczenia dostępu poprzez identyfikatory i hasła (polityka haseł Active Directory),
- restrykcje dotyczące zmian haseł co 14 dni,
- hasła dostępowe powinno składać się z min. 8 znaków alfanumerycznych (w przypadku braku możliwości wprowadzenia hasła 8 – znakowego należy stosować dodatkowe zabezpieczenia takie jak np. krótsze restrykcje dotyczące zmiany haseł),
- zabezpieczenie dostępu do stanowisk komputerowych poprzez hasło w BIOS-ie,
- zainstalowane wygaszacze ekranu z automatyczną blokadą profilu użytkownika.

---

11). Zarządzanie danymi osobowymi

Hasło powinno składać się z min. 8 znaków alfanumerycznych. Hasła dostępowe powinny być chronione i nie należy przekazywać haseł innym pracownikom.
Dostęp do danych osobowych możliwy jest tylko w godzinach urzędowania firmy tj. od 7:00 do 17:00. Po opuszczeniu stanowiska pracy przez pracownika należy zablokować stanowisko uniemożliwiając dostęp do danych osobom nieupoważnionym. Wszelkie operacje na danych osobowych rejestrowane są w systemie poprzez odnotowanie danych: użytkownik, godz. wprowadzenia, data wprowadzenia, data modyfikacji itp.

Dane osobowe gromadzone w systemie są archiwizowane zgodnie z harmonogramem przewidującym codzienne wykonywanie archiwów, tygodniowe, miesięczne i roczne. Archiwa danych przechowywane są w szafach pancernych kat. C – ognioodpornych i antywłamaniowych.
Zapewnienie środków ochrony fizycznej poprzez system kontroli dostępu do pomieszczeń.
Istnieją procedury w przypadku zaistnienia klęski żywiołowej lub katastrofy.
Dane osobowe chronione są oprogramowaniem antywirusowym Symantec Antyvirus Corporate Edition oraz sprzętowym firewall uniemożliwiającym dostęp z sieci publicznej osobom nieupoważnionym…..

22). Sposób przepływu danych

Protokoły teletransmisyjne: TCP/IP
Protokoły bezpieczeństwa: AES, 3DES, RSA, DSA, X.509

Pracownicy mobilni wykorzystują VPN szyfrowany 3DES

……..