ZATWIERDZAM
Prezes Zarządu
Dyrektor Naczelny

mgr inż. Andrzej Szymkiewicz

Spis treści:

Załącznik Nr 1/N* – Instrukcja tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania. Przechowywanie oraz transportowanie nośników z danymi i kopii zapasowych. Harmonogram wykonywania kopii zapasowych. Testowanie kopii zapasowych.

Załącznik Nr 2/N – Sposoby zabezpieczenia systemów informatycznych przed działaniem oprogramowania mającego na celu nieuprawniony dostęp oraz utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

***N** – informacje niejawne

DEKLARACJA

ZARZĄDU POŁUDNIOWEGO KONCERNU WĘGLOWEGO S.A.

Zarząd deklaruje, iż dołoży wszelkich starań oraz zapewni odpowiednie środki organizacyjno-finansowe, aby wdrożyć i utrzymywać na odpowiednio wysokim poziomie mechanizmy zabezpieczenia informacji i systemów informatycznych. Zamierzony, wysoki poziom ochrony informacji pragnie osiągnąć nie tylko poprzez dostosowanie działań do wymagań zawartych w obowiązujących przepisach, przyjęte dobre praktyki, ale również wdrażając system zarządzania bezpieczeństwem informacji w oparciu o Polską Normę PN-ISO/IEC 27001:2007.

Wiceprezes Zarządu
Dyrektor ds. Ekonomiczno-Finansowych

Prezes Zarządu – Dyrektor Naczelny

……

……

Wiceprezes Zarządu
Dyrektor ds. Technicznych

……

Wiceprezes Zarządu
Dyrektor ds. Handlowych

……

Wiceprezes Zarządu
Dyrektor ds. Pracy

……

CZĘŚĆ PODSTAWOWA

Politykę Bezpieczeństwa Informacji ustala i kształtuje Zarząd Południowego Koncernu Węglowego S.A.

Polityka Bezpieczeństwa Informacji Południowego Koncernu Węglowego S.A. jest całokształtem działań mających na celu zidentyfikowanie obiektów, zjawisk i działań, których celem jest ochrona informacji, a w szczególności ochrona danych osobowych.

Bezpieczeństwo informacji oznacza, że jest ona chroniona przed wieloma różnymi zagrożeniami w taki sposób, aby zapewnić ciągłość prowadzenia działalności oraz zminimalizować straty spowodowane zniszczeniem, utratą bądź „wyciekiem" informacji do osób i instytucji nieupoważnionych.

Zasady ochrony danych osobowych ustanowione Dyrektywą 95/46/EC wprowadzone zostały do polskiego porządku prawnego USTAWĄ z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2002r. Nr 101, poz. 926 ze zmianami).
Ustawa o ochronie danych osobowych wprowadziła szczegółowe normy prawne służące ochronie danych osobowych w Polsce, a od dnia 1 maja 2004r., czyli wstąpienia Polski do Unii Europejskiej, przeniosła do polskiego porządku prawnego wszystkie zasady określone w Dyrektywie 95/46/WE Parlamentu Europejskiego i Rady.

Aktem wykonawczym do Ustawy o ochronie danych osobowych jest ROZPORZADZENIE 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 2004r. Nr 100, poz. 1024).

Ilekroć w dokumentacji jest mowa o **ustawie** bądź **rozporządzeniu** – rozumie się przez to ustawę i rozporządzenie o których mowa powyżej.

Wykaz podstawowych terminów i definicji używanych w Polityce Bezpieczeństwa Informacji oraz wykaz aktów prawnych, zawierających wymagania z zakresu bezpieczeństwa informacji stanowi Załącznik Nr 1 do niniejszego dokumentu.

Południowy Koncern Węglowy S.A., jako podmiot posiadający osobowość prawną jest w rozumieniu ustawy **ADMINISTRATOREM DANYCH.**
Administrator danych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zmianą, utratą, uszkodzeniem lub zniszczeniem.

Do obsługi systemu informatycznego służącego do przetwarzania danych osobowych, może być dopuszczona osoba posiadająca upoważnienie wydane przez Prezesa Zarządu – Dyrektora Naczelnego, po uprzednim złożeniu podpisu przez właściwego Członka Zarządu – Dyrektora Pionu. Upoważnienie to stanowi podstawę do rejestracji użytkownika w systemie informatycznym i odbywa się zgodnie z zapisami Załącznika Nr 5.
Jeżeli dochodzi do przetwarzania danych osobowych wyłącznie w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych, tj. z wyłączeniem przetwarzania w systemach informatycznych, Kierownik komórki organizacyjnej występuje o nadanie upoważnienia dla podległego mu pracownika do Prezesa Zarządu - Dyrektora Naczelnego. Wniosek powinien zawierać: imię i nazwisko pracownika, nr stały, stanowisko, komórkę organizacyjną, zakres przetwarzania danych osobowych oraz opinię Administratora Bezpieczeństwa Informacji.

Dokument Polityki Bezpieczeństwa Informacji posiada strukturę (dokument podstawowy i załączniki), pozwalającą na odzwierciedlenie w dokumentacji prowadzenia procesu ciągłego doskonalenia w obszarze bezpieczeństwa informacji.

Polityka Bezpieczeństwa Informacji składa się z części jawnej, przeznaczonej do zapoznania ogółu pracowników oraz niejawnej zaopatrzonej klauzulą „Zastrzeżone”.
Sposób przechowywania oraz udostępniania części niejawnej reguluje ustawa o ochronie informacji niejawnych.

Celem Polityki Bezpieczeństwa Informacji jest:

- ochrona danych osobowych z zachowaniem prywatności informacji dotyczących osób fizycznych,
- skuteczniejsze działania w odniesieniu do zagrożeń poufności, integralności, rozliczalności i dostępności przetwarzania danych,
- stałe podnoszenie jakości i wiarygodności wobec kontrahentów,
- zapewnienie zgodności z prawem i wymaganiami wynikającymi z umów,
- upowszechnienie wytycznych i standardów w obszarze bezpieczeństwa informacji wśród pracowników i kontrahentów,
- usprawnienia przepływu i dostępu do informacji przy jednoczesnym wzroście ich bezpieczeństwa,
- ochrona informacji tworzonej, przetwarzanej, przechowywanej i przesyłanej.

Pełnomocnik ds. Ochrony Danych Osobowych i Bezpieczeństwa Informacji Przedsiębiorstwa, który równocześnie pełni obowiązki **Administratora Bezpieczeństwa Informacji** odpowiada za stworzenie, wdrożenie i nadzorowanie standardów ochrony informacji wynikających z przepisów prawa oraz prowadzenie kontroli w każdym obszarze mającym wpływ na jej bezpieczeństwo.

Prezes Zarządu – Dyrektor Naczelny powołał Zarządzeniem nr 48/2006 **Zespół ds. bezpieczeństwa informacji** i określił zasady jego działania**.**

Zespół jest m.in. zobowiązany na bieżąco monitorować i aktywnie reagować na zachodzące zmiany, zarówno zewnętrzne jak i wewnętrzne mogące pośrednio lub bezpośrednio wpływać na zagrożenia zasobów informacyjnych Spółki.

Polityka Bezpieczeństwa Informacji jest na bieżąco nadzorowana i okresowo (co najmniej raz w roku) weryfikowana przez Zespół ds. bezpieczeństwa informacji.

W razie wystąpienia potrzeby wprowadzenia zmian, Kierownicy komórek organizacyjnych występują z wnioskiem do Pełnomocnika ds. Ochrony Danych Osobowych i Bezpieczeństwa Informacji Przedsiębiorstwa o wprowadzenie tych zmian do dokumentu.

Pełnomocnik dokonuje analizy wniosku i niezwłocznie zwołuje Zespół ds. bezpieczeństwa informacji, który analizuje i opracowuje konieczne zmiany i wnioskuje o ich zatwierdzenie przez Zarząd Spółki.

Wnioskodawca powinien otrzymać odpowiedź w formie pisemnej w razie nie przyjęcia proponowanych zmian wraz z uzasadnieniem.

Polityka Bezpieczeństwa Informacji w szczególności obejmuje zagadnienia:

- deklarację zaangażowania Zarządu Spółki w bezpieczeństwo informacji,
- zasady ochrony i koordynacji bezpieczeństwa informacji,
- zabezpieczenia fizycznego dostępu do informacji,
- zasady przyznawania/odbierania upoważnień do przetwarzania danych osobowych,
- zasady kontroli dostępu do informacji,
- zasady i mechanizmy ochrony systemów IT,
- zasady postępowania w przypadku zaistnienia incydentu bezpieczeństwa,
- zasady dotyczących przechowywania, transportowania, zabezpieczania i odtwarzania danych,
- zasady inwentaryzacji i klasyfikacji informacji,
- wytyczne do zawierania umów outsourcingowych,
- zasady publikacji informacji poprzez serwer WWW oraz prowadzenia korespondencji w systemie poczty elektronicznej,
- kary za nieprzestrzeganie zasad bezpieczeństwa.

Każdy pracownik powinien niezwłocznie zostać zapoznany przez bezpośredniego przełożonego z Polityką Bezpieczeństwa Informacji. Potwierdzeniem powyższego jest własnoręczny podpis dokumentu świadczący o przebytym instruktażu, zgodnie ze wzorem zawartym w Załączniku nr 15.

Dokument ten powinien zostać włączony do akt osobowych pracownika.

Kierownik komórki organizacyjnej, w ramach której jest odpowiedzialny za osobę trzecią, np. konsultanta, audytora, odbywającego praktykę i staż, przeprowadza instruktaż zapoznając w niezbędnym zakresie z Polityką Bezpieczeństwa Informacji te osoby.

Zapoznanie z Polityką Bezpieczeństwa Informacji i obowiązek przestrzegania jej zapisów stosuje się również do podmiotów zewnętrznych, których dostęp do określonych zasobów informacyjnych wynika z zawartych umów lub może wynikać z charakteru świadczonych usług. Zakres i sposób zapoznania wraz ze wskazaniem osób, które należy zapoznać, powinien być zawarty w postanowieniach umowy.

Dokument zapoznania, zgodnie z Załącznikiem Nr 15, należy przechowywać w zasobach danej komórki organizacyjnej**.**

Każda zawierana umowa powinna posiadać klauzulę o poufności danych uzyskanych w związku z realizacją umowy, np. **…….** umowy zobowiązuje się do

(druga strona)

zachowania poufności informacji, dokumentów i innych danych dotyczących Południowego Koncernu Węglowego S.A., a uzyskanych w związku z realizacją tej umowy.

Kierownicy komórek organizacyjnych pełnią rolę **właścicieli informacji.**

W celu ciągłego doskonalenia wiedzy z zakresu ochrony danych osobowych i bezpieczeństwa informacji przedsiębiorstwa przeprowadzane są szkolenia uzupełniające wiedzę pracowników.
Szkolenia te odbywają się również na pisemny wniosek zainteresowanych pracowników.
Szkolenie takie przeprowadza Administrator Bezpieczeństwa Informacji lub osoba przez niego wyznaczona.
W zależności od potrzeb, na wniosek Administratora Bezpieczeństwa Informacji, szkolenie może przeprowadzić instytucja zewnętrzna.

Oryginał dokumentu „Polityka Bezpieczeństwa Informacji" posiada Prezes Zarządu – Dyrektor Naczelny, Kierownik Wydziału Organizacyjno-Prawnego oraz Pełnomocnik ds. Ochrony Danych Osobowych i Bezpieczeństwa Informacji Przedsiębiorstwa.
Pełnomocnik nanosi zmiany w arkuszu aktualizacji oryginalnych dokumentów.

Postępowanie w przypadkach zaistnienia nadzwyczajnych zdarzeń oraz sytuacji kryzysowych reguluje „Procedura gotowości na wypadek awarii i reagowania na awarie" Zintegrowanego Systemu Zarządzania.

Realizacja zapisów zawartych w Polityce Bezpieczeństwa Informacji spoczywa na wszystkich pracownikach.

Osoby, które zostały upoważnione do przetwarzania danych osobowych oraz innych informacji, w tym prawnie chronionych, są obowiązane zachować w tajemnicy dane osobowe i inne informacje oraz sposoby ich zabezpieczenia.

Zabrania się przetwarzania danych osobowych niezgodnie z zapisami ustawy i obowiązujących aktów wykonawczych wydanych na jej podstawie.

Za naruszenia postanowień zawartych w Polityce Bezpieczeństwa Informacji mogą zostać zastosowane kary przewidziane w Regulaminie Pracy Południowego Koncernu Węglowego S.A. oraz sankcje karne wynikające z polskiego prawa.

Opracował:

……..
/Data, Podpis/

Rejestr zmian / Arkusz aktualizacji

Nr zmiany	Przedmiot zmiany	Data wprowa-dzenia zmiany	Opis zmiany	Podpis