I. Za naruszenie ochrony danych osobowych uznaje się przypadki, w których:

1. Stwierdzono naruszenie zabezpieczenia teleinformatycznego wpływającego na bezpieczeństwo danych osobowych.
2. Doszło do naruszenia bezpieczeństwa fizycznego wpływającego na bezpieczeństwo danych osobowych.
3. Doszło do nieuprawnionego przekazania lub przetwarzania danych osobowych.
4. Doszło do uszkodzenia lub zniszczenia zasobów danych osobowych.

II. Każdy pracownik Południowego Koncernu Węglowego S.A., który stwierdzi lub podejrzewa naruszenia ochrony danych osobowych lub innych informacji prawnie chronionych w systemie informatycznym zobowiązany jest do niezwłocznego poinformowania o tym Administratora Bezpieczeństwa Informacji.

Administrator Bezpieczeństwa Informacji wnosi do Administratora Systemów Informatycznych o niezwłoczne:

1. Poddanie szczegółowej analizie stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych czy innych informacji prawnie chronionych.
2. Zapisanie wszelkich informacji i okoliczności związanych z danym zdarzeniem.
3. Jeżeli zasoby systemu na to pozwalają, wygenerowanie i wydrukowanie wszystkich dokumentów i raportów (dowodów), które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania.
4. Przystąpienie do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu do informacji, itp.
5. Podjęcie odpowiedniego postępowania w celu ograniczenia dalszego, niepowołanego dostępu osób nieuprawnionych, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych poprzez:
    a) fizyczne odłączenie urządzeń i segmentów sieci, które umożliwiły lub mogły umożliwić dostęp do bazy danych,
    b) wylogowanie użytkownika podejrzanego o naruszenie ochrony danych,

c) zmianę hasła użytkownika poprzez którego uzyskano nielegalny dostęp do bazy danych w celu uniknięcia ponownej próby dostępu.

6. Przywrócenie normalnego działania systemu z zachowaniem wszelkich dostępnych środków zapewniających bezpieczeństwo danych.
7. Poddanie szczegółowej analizie ryzyka zaistnienia podobnych incydentów wraz z zastosowaniem właściwej profilaktyki, aby w przyszłości nie dochodziło do podobnych zdarzeń.
8. Przeprowadzenia szkolenia użytkownika lub grupy użytkowników mających wpływ za zaistniałe zdarzenie.

III. Każdy pracownik Południowego Koncernu Węglowego S.A., który stwierdzi lub podejrzewa naruszenia ochrony danych osobowych lub innych informacji prawnie chronionych w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych zobowiązany jest do niezwłocznego poinformowania o tym Administratora Bezpieczeństwa Informacji oraz Kierownika właściwej komórki organizacyjnej nadzorującej zbiory jak wyżej.

Kierownik komórki organizacyjnej, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony danych osobowych czy innych informacji prawnie chronionych zobowiązany jest do niezwłocznego:

1. Poddania szczegółowej analizy stanu nadzorowanej dokumentacji w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych czy innych informacji prawnie chronionych.
2. Zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu lub samodzielnym wykryciu tego faktu.
3. Przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń zasobów, sposobu dostępu do informacji, itp.

4. Podjęcia odpowiedniego postępowania w celu ograniczenia dalszego, niepowołanego dostępu osób nieuprawnionych, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych poprzez:
    a) podjęcia odpowiedniego postępowania w celu ograniczenia dalszego, niepowołanego dostępu osób nieuprawnionych, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych,
    b) odsunięcie od wykonywania pracy pracownika, który przyczynił się lub był odpowiedzialny za zaistniałe zdarzenie.
5. Przywrócenia normalnego funkcjonowania komórki organizacyjnej z zachowaniem wszelkich dostępnych środków zapewniających bezpieczeństwo danych.
6. Poddanie szczegółowej analizie ryzyka zaistnienia podobnych incydentów wraz z zastosowaniem właściwej profilaktyki, aby w przyszłości nie dochodziło do podobnych zdarzeń.
7. Przeprowadzenia szkolenia pracownika lub grupy pracowników mających wpływ za zaistniałe zdarzenie.

IV. Postanowienia końcowe.

1. Administrator Bezpieczeństwa Informacji o każdym naruszeniu ochrony danych osobowych powiadamia niezwłocznie Administratora Danych oraz prowadzi rejestr naruszeń ochrony danych osobowych.
2. Jeżeli w wyniku przeprowadzenia analizy zaistnienia incydentu stwierdzono zaniedbanie ze strony pracownika, Administrator Bezpieczeństwa Informacji ujawni Zarządowi nazwisko osoby/osób, jak również poinformuje o ewentualnym złamaniu prawa.
3. Zarząd może podjąć kroki dyscyplinarne, a w uzasadnionych przypadkach złamania prawa zdecydować o poinformowaniu organów ścigania.

-Koniec-