I. W Południowym Koncernie Węglowym S.A. należy stosować środki techniczne i organizacyjne zapewniając poufność, dostępność, rozliczalność i integralność danych.

Poufność – to właściwość zapewniająca, że do informacji mają dostęp wyłącznie upoważnione osoby (podmioty).

Dostępność – to zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne.

Rozliczalność – to właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

Integralność – to właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

II. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, dostępności, rozliczalności i integralności danych zostało poprzedzone analizą zagrożeń związanych z przetwarzaniem danych w obszarach, przeprowadzoną przez Pełnomocnika ds. Ochrony Danych Osobowych i Bezpieczeństwa Informacji Przedsiębiorstwa:

1. **Budynki i pomieszczenia**: włamanie, pożar, zalanie, katastrofy budowlane, katastrofy żywiołowe, nieuprawniony dostęp do pomieszczeń.
2. **Systemy operacyjne, sprzęt komputerowy, serwery, komputery osobiste**: wyłączenie zasilania, włamanie do systemu, skasowanie, zmiana lub skopiowanie danych, zagrożenie wirusami, zmiana konfiguracji, unieruchomienie serwera, nieuprawniony dostęp do poczty, dostęp do Internetu, kradzież, pożar, zalanie, nieuprawniony dostęp do pomieszczeń, uszkodzenie lub zniszczenie sprzętu.
3. **Systemy baz danych i programy (aplikacje)**: włamanie do systemu, skasowanie, zmiana lub skopiowanie danych, zagrożenie wirusami, zmiana konfiguracji użytkowników i ich uprawnień do poszczególnych modułów i funkcji, dostęp do systemu z poziomu aplikacji.

4. **Urządzenia sieciowe**: uszkodzenie na skutek niewłaściwej eksploatacji, uszkodzenie na skutek nieprzewidzianych zdarzeń i sytuacji kryzysowych, podsłuch, zmiana konfiguracji urządzeń, nieuprawniony dostęp do zasobów sieciowych, awaria (uszkodzenie) łączy teletransmisyjnych.
5. **Organizacyjne i kadrowe**: nieuprawniony dostęp, świadome i nieświadome zniszczenie lub uszkodzenie sprzętu, świadome i nieświadome zniszczenie danych.

III. Dla obszarów sprecyzowanych w punkcie II zastosowano lub należy zastosować środki techniczne i organizacyjne pozwalające na wyeliminowanie bądź ograniczenie prawdopodobieństwa wystąpienia zagrożeń :

1. **Budynki i pomieszczenia**: ochrona budynku, ewidencja wejść, ewidencja wjazdów, kontrole osób trzecich przy wyjściu/wyjeździe z terenu PKW S.A., monitorowanie budynków i pomieszczeń, listy osób uprawnionych do wskazanych pomieszczeń, stosowanie wideo i domofonów, systemy przeciwpożarowe, systemy alarmowe, systemy nadzoru i kontroli, przyrządy pomiarowe i aparatura pomiarowa, stosowanie klimatyzacji w serwerowniach, weryfikowanie i aktualizacja właściwych procedur i instrukcji.
2. **Systemy operacyjne, sprzęt komputerowy, serwery, komputery osobiste**: uwierzytelnianie i autoryzacja użytkowników, zabezpieczenia fizyczne szaf, biurek i pomieszczeń, kopie zapasowe przechowywane w pomieszczeniach zamkniętych z kontrolą dostępu i monitoringiem przeciwpożarowym i temperatury, stosowanie sprzętu rezerwowego, testowanie sprzętu rezerwowego, szyfrowane połączeń, korzystanie z zapory połączenia internetowego, pobieranie aktualizacji oprogramowania systemowego, aktualne programy antywirusowe, używanie silnych haseł, przeglądanie zasobów Internetu z zachowaniem środków ostrożności, system antywirusowy poczty elektronicznej, regularne wykonywanie kopii zapasowych, testowanie kopii zapasowych, ochrona danych archiwizowanych, dodatkowo dla komputerów przenośnych szyfrowanie danych na dysku, zabezpieczenie przed kradzieżą, ochrona w czasie

podróży, stosowanie UPS'ów, stosowanie właściwego nadzoru i kontroli, weryfikowanie i aktualizacja właściwych procedur i instrukcji.

3. **Systemy baz danych i programów**: stosowanie środków j.w.
4. **Urządzenia sieciowe, sieć logiczna i elektryczna, zdalny dostęp**: gniazda elektryczne z kluczem przyłączeniowym, ochrona przepięciowa i przeciwporażeniowa, kable prowadzone w miejscach o ograniczonym dostępie, dostęp do konfiguracji urządzeń tylko z określonych miejsc, konfiguracja urządzeń z wykorzystaniem protokołów szyfrowanych, stosowanie archiwizacji konfiguracji urządzeń, niewykorzystane gniazda urządzeń sieciowych właściwie skonfigurowane, dla połączeń zdalnych silne protokoły szyfrowania, weryfikacja i autoryzacja użytkowników na wielu poziomach, stosowanie sprzętu i oprogramowania dla monitorowania logów, serwis łącz, urządzenia zapasowe, testowanie sprzętu i urządzeń zapasowych, stosowanie właściwego nadzoru i kontroli, weryfikowanie i aktualizacja właściwych procedur i instrukcji.
5. **Organizacyjne i kadrowe**: opracowanie polityki i koncepcji bezpieczeństwa, przestrzeganie odpowiednich procedur i instrukcji, szkolenie pracowników, stosowanie polityki „czystego biurka i czystego ekranu".

- Koniec -