Wypis z protokołu nr 5//2019
z posiedzenia Zarządu Spółki Dolnośląskie
Przedsiębiorstwo Napraw Infrastruktury
Komunikacyjnej DOLKOM
spółka z ograniczoną odpowiedzialnością.
z dnia 28.01.2019 r.

Uchwała nr 10 /2019

Zarządu Spółki Dolnośląskie Przedsiębiorstwo Napraw Infrastruktury Komunikacyjnej DOLKOM spółka z ograniczoną odpowiedzialnością
z dnia 28.01.2019r.

w sprawie przyjęcia nowej treści **Polityki Bezpieczeństwa Informacji**

Na podstawie § 12 ust. 1 i 2 Umowy Spółki oraz § 10 ust. 20 Regulaminu Zarządu Dolnośląskiego Przedsiębiorstwa Napraw Infrastruktury Komunikacyjnej DOLKOM sp. z o.o. Zarząd Spółki uchwala, co następuje:

§ 1

Przyjmuje do stosowania w Spółce dokument pt. Polityka Bezpieczeństwa Informacji w Dolnośląskim Przedsiębiorstwie Napraw Infrastruktury Komunikacyjnej DOLKOM sp. z o.o., stanowiący załącznik nr 1 do niniejszej uchwały.

§ 2

W związku z § 1 traci moc Uchwała Nr 55/2016 Zarządu DOLKOM sp. z o.o. z dnia 06.04.2016r. w sprawie przyjęcia Polityki Bezpieczeństwa Informacji w Dolnośląskim Przedsiębiorstwie Napraw Infrastruktury Komunikacyjnej DOLKOM sp. z o.o. we Wrocławiu.

§ 3

Uchwała obowiązuje z dniem podjęcia.

Głosowanie przeprowadzono w trybie jawnym/tajnym*
Ilość obecnych: 3 ilość głosów „za" 3 ilość głosów „przeciw" 0 ilość wstrzymujących się: 0

PREZES ZARZĄDU
Andrzej Gola

Załącznik

do Uchwały Nr 10 /2019

Zarządu DOLKOM sp. z o.o.

z dnia 28.01. 2018 roku

POLITYKA BEZPIECZEŃSTWA INFORMACJI

W DOLNOŚLĄSKIM PRZEDSIĘBIORSTWIE NAPRAW INFRASTRUKTURY KOMUNIKACYJNEJ DOLKOM SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ WE WROCŁAWIU

§ 1

Cele

1. Celem Polityki Bezpieczeństwa Informacji (dalej PBI) jest zapewnienie:
   a) integralności i poufności,
   b) legalności,
   c) rozliczalności,
   d) dostępności,

   informacji przetwarzanych w Dolnośląskim Przedsiębiorstwie Napraw Infrastruktury Komunikacyjnej DOLKOM sp. z o.o. (dalej **Spółka**) poprzez ustalenie zasad postępowania Spółki w zakresie bezpieczeństwa przetwarzania informacji.
2. Celem PBI jest również zapewnienie mechanizmów ochrony informacji, komplementarnych z zasadami i wymogami prawnymi dotyczącymi ochrony danych osobowych.

§ 2

Postanowienia ogólne

1. PBI określa metody i zasady ochrony oraz zapewnienia bezpieczeństwa informacji w Spółce, stanowiąc wyraz zdecydowanej woli Zarządu Spółki zapewnienia właściwej ochrony informacji i deklarację wsparcia dla odpowiednich działań w tym zakresie.
2. Spółka uznaje za zasadne i celowe dokonywanie inwestycji w obszarze bezpieczeństwa informacji, a w szczególności w sprawność i bezpieczeństwo infrastruktury teleinformatycznej.
3. PBI stanowi podstawę do opracowania i wdrożenia dokumentów zawierających wymagania dla konkretnych kategorii informacji, a także określających warunki, jakie musi spełniać przetwarzanie danych w systemie teleinformatycznym i tradycyjnym (opartym na dokumentacji papierowej), z uwzględnieniem aspektów prawnych ochrony informacji i stabilności systemów teleinformatycznych.

§ 3

Definicje pojęć

Dla potrzeb PBI następujące pojęcia oznaczają:

1) **bezpieczeństwo informacji** – stan zapewniający informacjom przetwarzanym w Spółce poufność, integralność, dostępność i rozliczalność,
2) **bezpieczeństwo fizyczne** - zespół odpowiednio dobranych środków organizacyjnych, technicznych (mechanicznych, elektronicznych i budowlanych) oraz personalnych zapewniających skuteczną ochronę fizyczną (materialną) informacji przetwarzanych w Spółce, w tym nośników, na których informacje są utrwalone,
3) **bezpieczeństwo osobowe** - zespół odpowiednio dobranych środków organizacyjnych i proceduralnych uwzględniających aspekt bezpieczeństwa informacji, stosowanych w organizacji pracy personelu Spółki, w szczególności w przydzielaniu obowiązków i uprawnień pracowników,
4) **bezpieczeństwo teleinformatyczne** – ochrona informacji przetwarzanych za pomocą systemów teleinformatycznych przed nieuprawnionym dostępem, a w tym odczytem, kopiowaniem, modyfikacją lub zniszczeniem,
5) **dokument** – każdy nośnik, na którym utrwalono w sposób w pełni lub częściowo czytelny jakikolwiek rodzaj informacji, w szczególności papier, mikrofilm, negatyw fotograficzny, fotografia, przenośny nośnik danych utrwalanych w postaci cyfrowej, taśma elekromagnetyczna,
6) **dostępność informacji** – możliwość przetwarzania informacji, w szczególności poprzez zapoznanie się z jej treścią, przez podmiot upoważniony,

7) **informacja** – wszelkiego rodzaju treści wyrażone w jakikolwiek odczytywalny (zrozumiały) sposób, w jakimkolwiek dokumencie,
8) **informacje prawnie chronione** - informacje zakwalifikowane do jednej z grup od I do IV w § 4,
9) **integralność informacji** – zabezpieczenie informacji przed nieuprawnionym (niedozwolonym lub niezgodnym z prawem) przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem,
10) **jednostka organizacyjna** - jednostka organizacyjna wchodząca, zgodnie z regulaminem organizacyjnym Spółki, w skład jej struktury organizacyjnej,
11) **komórka organizacyjna** – wydzielona organizacyjnie część jednostki organizacyjnej,
12) **materiał** - dokument, jak też przedmiot lub dowolna jego część, a zwłaszcza urządzenie,
13) **poufność informacji** – zabezpieczenie informacji przed nieuprawnionym dostępem (pozyskaniem),
14) **przetwarzanie informacji (danych)** - operacja lub zestaw operacji wykonywanych wobec informacji (na danych) lub zestawach informacji (danych) w sposób zautomatyzowany lub niezautomatyzowany, jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,
15) **rozliczalność informacji** – stan umożliwiający jednoznaczną identyfikację osoby dokonującej czynności przetwarzania oraz potwierdzenie prawidłowości formalno-prawnej takiego przetwarzania,
16) **sieć teleinformatyczna** – organizacyjne i techniczne połączenie stosowanych w Spółce systemów teleinformatycznych,
17) **system przetwarzania informacji** – system (manualny albo informatyczny), który tworzą urządzenia, narzędzia, metody postępowania i procedury stosowane przez wyspecjalizowanych pracowników Spółki w sposób zapewniający przetwarzanie informacji.

§ 4

Klasyfikacja informacji

1. W Spółce ustala się następującą klasyfikacje przetwarzanych informacji:

grupa I	informacje niejawne w rozumieniu ustawy z dnia 05.08.2010r. o ochronie informacji niejawnych (Dz.U. z 2018r., poz. 412, t.j.)
grupa II	dane osobowe w rozumieniu ustawy z dnia 10.05.2018r. o ochronie danych osobowych (Dz. U. z 2018r. poz. 1000)
grupa III	tajemnica przedsiębiorstwa (przedsiębiorcy) DOLKOM sp. z o.o. w rozumieniu ustawy z dnia 16.04.1993r. o zwalczaniu nieuczciwej konkurencji (Dz.U. z 2018r. poz. 419, t.j.) oraz ustawy z dnia 06.09.2001r. o dostępie do informacji publicznej (Dz.U. z 2016r. poz. 1764, t.j.)
grupa IV	informacje uzyskane przez Spółkę w związku z realizacją umów, współpracą z podmiotami trzecimi lub innym rodzajem aktywności w ramach prowadzonej działalności gospodarczej – jeżeli ich ochrona wynika z zawartych tak umów lub przepisów powszechnie obowiązujących
grupa V	informacje publicznie dostępne (jawne)

2. Za właściwe zakwalifikowanie informacji do odpowiedniej grupy odpowiada jej autor.
3. Zasady i wytyczne ujęte w PBI mogą być rozwijane i uszczegóławiane w dodatkowych

dokumentach wewnętrznych Spółki, odpowiednio dla poszczególnych grup informacji.

4. PBI jest dokumentem jawnym, podlegającym fizycznemu udostępnieniu w siedzibie Biura Zarządu Spółki albo (na wniosek zainteresowanego) w innej formie, w szczególności elektronicznej.
5. Zapoznanie się z PBI potwierdza pisemnie, przed rozpoczęciem zatrudnienia (współpracy / stażu / praktyki), wg wzoru stanowiącego załącznik do PBI:
   a) pracownik Spółki, z którym łączy Spółkę umowa o pracę w rozumieniu Kodeksu pracy,
   b) współpracownik Spółki, z którym łączy Spółkę umowa inna niż umowa o pracę w rozumieniu Kodeksu pracy,
   c) praktykant / stażysta.
6. Przed odebraniem pisemnego potwierdzenia zapoznania się z PBI pracownik Spółki weryfikuje posiadanie przez osobę potwierdzającą jednego ze statusów prawnych wskazanych w ust. 5 lit. a) – lit. c).

§ 5

Zasoby Spółki podlegające ochronie

Do zasobów zidentyfikowanych w Spółce podlegających ochronie w kontekście bezpieczeństwa informacji należą:

1) zasoby personalne (pracownicy, ich kwalifikacje, umiejętności, wiedza, zdolności itp.),
2) zasoby finansowe (kapitał, papiery wartościowe),
3) zasoby majątkowe (budynki, maszyny i wszelkiego rodzaju sprzęt),
4) zasoby informacyjne (sprawozdania, statystyki, prognozy, oferty, cenniki itp.).

§ 6

Bezpieczeństwo informacji

1. Bezpieczeństwo osobowe.
   a) Dla każdej grupy informacji wymagania dotyczące bezpieczeństwa osobowego definiowane są w politykach lub instrukcjach bezpieczeństwa tej grupy informacji oraz, w razie konieczności, w innych dokumentach szczegółowych.
   b) Wymagania dotyczące bezpieczeństwa osobowego w zakresie dostępu do systemów i sieci teleinformatycznych są zdefiniowane w polityce (instrukcji) bezpieczeństwa teleinformatycznego oraz dokumentach szczegółowych i uregulowaniach wewnętrznych właściwych dla danego systemu lub sieci teleinformatycznej.
2. Bezpieczeństwo fizyczne.
   a) Wymagania bezpieczeństwa fizycznego określają odrębne uregulowania wewnętrzne Spółki, w szczególności instrukcja w sprawie organizacji ochrony fizycznej informacji prawnie chronionych.
   b) Organizacja i zasady funkcjonowania ochrony fizycznej podlegają ustaleniu odrębnie, w szczególności w umowach świadczenia usług ochrony fizycznej mienia.
3. Bezpieczeństwo teleinformatyczne.
   Bezpieczeństwo teleinformatyczne jest zapewniane poprzez wdrożenie w Spółce systemu zarządzania bezpieczeństwem teleinformatycznym. Zasady i mechanizmy systemu są ustalane w polityce bezpieczeństwa teleinformatycznego i, w razie konieczności innych regulacjach odrębnych.
4. Bezpieczeństwo dokumentów.
   a) Sposób ochrony dokumentów, proporcjonalny do poufności informacji w nich zawartych, wartości tych informacji i wymagań bezpieczeństwa jest zapewniany

uregulowaniami wewnętrznymi Spółki, a w tym regulaminem pracy oraz zobowiązaniami do zachowania poufności.

b) Sposób zarządzania dostępem do dokumentów, oparty na zasadzie „wiedzy uzasadnionej" zakłada, że pracownik może uzyskać dostęp do informacji prawnie chronionej:
   a. o ile jest do tego uprawniony zgodnie z obowiązującymi przepisami,
   b. w zakresie niezbędnym do wykonywania jego obowiązków pracowniczych.

c) Integralność, poufność i rozliczalność informacji utrwalonych w dokumentach zapewniane są przez system ewidencji obiegu dokumentów, pozwalający na ustalenie lokalizacji oznaczonego dokumentu w ramach struktury organizacyjnej Spółki.

5. Bezpieczeństwo współpracy zewnętrznej.
   a) Podmiot zewnętrzny ubiegający się o zawarcie ze Spółką umowy, której realizacja może wiązać się z dostępem do informacji przetwarzanych w Spółce, ma obowiązek:
      a. zapoznania się z PBI zgodnie z § 4 ust. 5,
      b. zapewnienia należytej, zgodnej z PBI i innymi odpowiednimi regulacjami, ochrony informacji, do których uzyska dostęp,
      c. zapewnić, aby każda osoba lub podmiot, działający w jego imieniu, dopełnił obowiązków opisanych w pkt a i pkt b.
   b) Realizacja umowy zawartej z podmiotem zewnętrznym podlega bieżącemu nadzorowi m.in. w kontekście bezpieczeństwa informacji. Umowa powinna zawierać zapisy, że uchybienia w zapewnieniu przez podmiot zewnętrzny lub podmioty działające w jego imieniu i na jego rzecz, wymaganego bezpieczeństwa informacji stanowią jej rażące (istotne) naruszenie. Umowa powinna zawierać zapisy, że rażące (istotne) jej naruszenie upoważnia Spółkę do rozwiązania umowy w trybie natychmiastowym, żądania kary umownej oraz odszkodowania uzupełniającego.

§ 7
Wdrożenie i odpowiedzialność

1. Odpowiedzialność za realizację PBI ponosi:
   a) każdy kierownik jednostki organizacyjnej lub komórki organizacyjnej Spółki – w zakresie związanym z czynnościami realizowanymi przez niego osobiście oraz z czynnościami nadzoru (nadrzędności),
   b) każdy pracownik Spółki – w zakresie realizacji jego obowiązków pracowniczych,
   c) podmiot zewnętrzny, z którym łączy Spółkę umowa cywilnoprawna – w zakresie wynikającym z realizacji tej umowy.
2. Odpowiedzialność opisana w ust. 1 nie uchyla ewentualnej odpowiedzialności za naruszenie tajemnic prawnie chronionych, wynikającej z przepisów powszechnie obowiązujących.

§ 8
Postanowienia końcowe

PBI nie uchyla, ani nie modyfikuje zasad ochrony informacji oraz zapewnienia bezpieczeństwa informacji, wynikających z odrębnych przepisów.

Załącznik

Wzór wykazu pracowników, współpracowników i stażystów (praktykantów)
Dolnośląskiego Przedsiębiorstwa Napraw Infrastruktury Komunikacyjnej DOLKOM sp. z o.o.
którzy zapoznali się z Polityką Bezpieczeństwa Informacji (PBI),
przyjmując ją wiążąco do stosowania.

Lp.	Imię i nazwisko	Stanowisko/ przedsiębiorstwo	Data	Potwierdzenie zapoznania się z PBI