POLSKA IZBA INŻYNIERÓW BUDOWNICTWA

POLSKA IZBA INŻYNIERÓW BUDOWNICTWA

(zwana dalej PIIB)
ul. Mazowiecka 6/8
00-048 Warszawa

POLITYKA BEZPIECZEŃSWA

Data i miejsce sporządzenia dokumentu:	1 / 03 / 2012 r. (dd/mm/rrrr)
Ilość stron:	29
Organ zatwierdzający:	Krajowa Rada Polskiej Izby Inżynierów Budownictwa

Zatwierdzona do użytku Uchwała Prezydium Krajowej Rady PIIB …… z dnia …….

potwierdzonej Uchwała Krajowej Rady PIIB……z dnia ……..

Parafa:	

SPIS TREŚCI

Parafa:	

1. WSTĘP

1.1. INFORMACJE OGÓLNE

Niniejszy dokument Polityki Bezpieczeństwa został opracowany przez Administratora Danych – Polską Izbę Inżynierów Budownictwa, w celu zapewnienia zgodności przetwarzania danych osobowych z polskim ustawodawstwem.

Polityka Bezpieczeństwa wraz z Instrukcją Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych stanowi dokumentację przetwarzania danych osobowych w rozumieniu § 1 pkt 1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. 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. Nr 100, poz. 1024 z późn. zm.).

Polityka Bezpieczeństwa obowiązuje od dnia 1 / 03 / 2012 (dd/mm/rrrr). Wszelkie wątpliwości dotyczące sposobu interpretacji postanowien niniejszego dokumentu Polityki Bezpieczeństwa, powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.

Każda osoba mającą dostęp do danych osobowych z upoważnienia Administratora Danych, została zapoznana z Polityką Bezpieczeństwa i zobowiązana do jej przestrzegania w zakresie wynikającym z przydzielonych zadań. Dotyczy to w szczególności pracowników zatrudnionych przez Administratora Danych. Osoby o których mowa, złożyły na piśmie oświadczenie o zapoznaniu się z treścią Polityki Bezpieczeństwa oraz zobowiązały się do stosowania zawartych w niej postanowień.

1.2. CEL PRZYGOTOWANIA POLITYKI BEZPIECZEŃSTWA

Podstawowym celem przyświecającym przygotowaniu i wdrożeniu dokumentu Polityki Bezpieczeństwa jest zapewnienie zgodności działania Polskiej Izby Inżynierów Budownictwa i jej organów z ustawą o ochronie danych osobowych oraz jej rozporządzeniami wykonawczymi. Dokument Polityki Bezpieczeństwa został opracowany na podstawie przepisów zawartych w następujących aktach prawnych:

1) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. 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. Nr 100, poz. 1024 z późn. zm.),
2) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),
3) ustawa z dnia 15 grudnia 2000 r. o samorządach zawodowych architektów, inżynierów budownictwa oraz urbanistów (Dz. U. z 2001 r. Nr 5 poz. 42 z późn. zm.),
4) Statut Polskiej Izby Inżynierów Budownictwa,
5) Regulamin Krajowej Rady Polskiej Izby Inżynierów Budownictwa.

Należy przez powyższe rozumieć w szczególności realizację w niniejszym dokumencie wymogu opisania sposobu przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. Zadaniem Polityki Bezpieczeństwa jest także określenie podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz wymagań w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.

Parafa:	

1.3. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA ORAZ ZAKRES ZASTOSOWANIA

Dokument Polityki Bezpieczeństwa opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem. Jest to zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz Polskiej Izby Inżynierów Budownictwa. Polityka Bezpieczeństwa, odnosi się całościowo do problemu zabezpieczenia danych osobowych tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych. Na Politykę Bezpieczeństwa składają się następujące informacje:

1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,
2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
4) sposób przepływu danych pomiędzy poszczególnymi systemami,
5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Politykę Bezpieczeństwa stosuje się do wszelkich czynności, stanowiących w myśl ustawy o ochronie danych osobowych, przetwarzanie danych osobowych. Bez względu na źródło pochodzenia danych osobowych, ich zakres, cel zebrania, sposób przetwarzania lub czas przetwarzania, stosowane są zasady przetwarzania danych osobowych ujęte w niniejszym dokumencie Polityki Bezpieczeństwa. Rygorowi Polityki Bezpieczeństwa podlegają także dane powierzone Polskiej Izbie Inżynierów Budownictwa do przetwarzania na podstawie pisemnej umowy powierzenia przetwarzania danych osobowych oraz dane osobowe, których Polska Izba Inżynierów Budownictwa jest odbiorcą w rozumieniu ustawy o ochronie danych osobowych.

Parafa:	

1.4. WYJAŚNIENIE TERMINÓW UŻYWANYCH W DOKUMENCIE POLITYKI BEZPIECZEŃSTWA

1) **rozporządzenie** – rozumie się przez to rozporządzenie ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r. 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. Nr 100, poz. 1024 z późn. zm.), zwane dalej „rozporządzeniem",
2) **ustawa** - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133 poz. 883 z późn. zm.), zwaną dalej „ustawą",
3) **administrator danych** – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3 ustawy o ochronie danych osobowych, decydujące o celach i środkach przetwarzania danych osobowych, w rozumieniu niniejszej **Polityki Bezpieczeństwa** administratorem danych osobowych jest **Polska Izba Inżynierów Budownictwa** z siedzibą: ul. Mazowiecka 6/8, 00-048 Warszawa,
4) **dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
5) **hasło** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
6) **identyfikator użytkownika** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
7) **instrukcja zarządzania systemem informatycznym** – dokument instrukcji zarządzania systemem informatycznym w rozumieniu § 1 pkt 1 rozporządzenia, zwaną dalej „instrukcją",
8) **integralność danych** - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
9) **odbiorca danych** - rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
    a. osoby, której dane dotyczą,
    b. osoby upoważnionej do przetwarzania danych,
    c. przedstawiciela, o którym mowa w art. 31a ustawy o ochronie danych osobowych,
    d. podmiotu, o którym mowa w art. 31 ustawy o ochronie danych osobowych,
    e. organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
10) **państwo trzecie** - rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego,

Parafa:	

11) **Polityka Bezpieczeństwa** – dokument Polityki Bezpieczeństwa w rozumieniu § 1 pkt 1 rozporządzenia, zwaną dalej „Polityką”,
12) **poufność danych** - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
13) **przetwarzanie danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
14) **raport** - rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,
15) **rozliczalność** - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
16) **sieć publiczna** - rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852 z późn. zm.),
17) **sieć telekomunikacyjna** - rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852 z późn. zm.),
18) **system informatyczny** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
19) **teletransmisja** - rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,
20) **usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
21) **uwierzytelnianie** - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
22) **zabezpieczenie danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
23) **zbiór danych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
24) **zgoda osoby, której dane dotyczą** - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści,

Parafa:	

2. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

2.1. INFORMACJE OGÓLNE

Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami Ustawy, Rozporządzenia, Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych odpowiadają w PIIB:

1. Administrator Danych,
2. Administrator Bezpieczeństwa Informacji,
3. Administrator Systemów Informatycznych,
4. Każda osoba wykonująca pracę bądź świadcząca usługi na rzecz PIIB, która uzyskała upoważnienie do przetwarzania danych osobowych.

2.2.1. ADMINISTRATOR DANYCH

1. Polska Izba Inżynierów Budownictwa z siedzibą: ul. Mazowiecka 6/8, 00-048 Warszawa, powołana na mocy ustawy z dnia 15 grudnia 2000 r. o samorządach zawodowych architektów, inżynierów budownictwa i urbanistów (Dz. U. 2001 r. Nr 5, poz.42 z późn. zm.), wpisana do Krajowego Rejestru Urzędowego Podmiotów Gospodarki Narodowej pod numerem REGON 015314008, identyfikująca się numerem NIP 525–22-54-990 jest Administratorem Danych. W imieniu Administratora Danych obowiązki określone w Ustawie i Rozporządzeniu pełni Krajowa Rada w imieniu której działają Prezes i sekretarz Krajowej Rady. Na dzień wejścia w życie Polityki Bezpieczeństwa funkcje te pełnią następujące osoby:

- Andrzej Roch Dobrucki - Prezes
- Ryszard Dobrowolski – Sekretarz

Zmiana osób pełniących funkcję Prezesa i sekretarza Krajowej Rady nie wymaga zmiany Polityki bezpieczeństwa.

Administrator Danych, poprzez osoby go reprezentujące, każdorazowo wyraża zgodę oraz ostateczną akceptację na wszystkie działania Administratora Bezpieczeństwa Informacji, w które zaangażowane są podmioty trzecie. Do zaakceptowania działań Administratora Bezpieczeństwa Informacji, wystarczająca jest zgoda w/w osób, wyrażona w formie pisemnej.

Parafa:	

2.2.2. ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

1. Funkcję Administratora Bezpieczeństwa Informacji (ABI) pełni w PIIB Adam Kuśmierczyk .

2. Zmiana osoby pełniącej funkcję Administratora Bezpieczeństwa Informacji następuje na skutek pisemnej decyzji Administratora Danych - Krajowej Rady podpisanej przez Prezesa i sekretarza Krajowej Rady.

3. Do uprawnień i obowiązków Administratora Bezpieczeństwa Informacji należy, w szczególności:

a) zgłaszanie zbiorów danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych oraz zgłaszanie wniosków o wykreślenie zbioru z rejestru zbiorów danych prowadzonego przez ww. organ, jeśli zachodzi konieczność dokonania takich czynności w odniesieniu do danego zbioru danych osobowych,

b) wnioskowanie do Dyrektora Krajowego Biura PIIB o konieczności nadania pracownikowi upoważnienia do przetwarzania danych osobowych w systemach informatycznych,

c) stały nadzór nad treścią Polityki Bezpieczeństwa, Instrukcji Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych oraz innymi dokumentami związanymi z ochroną danych osobowych stosowanych w PIIB oraz aktualizacja i modyfikacja w/w dokumentów,

d) udzielanie Generalnemu Inspektorowi Ochrony Danych Osobowych lub innym organom odpowiedzi i wyjaśnień w sprawie zbiorów danych osobowych przetwarzanych w PIIB,

e) udział w kontrolach prowadzonych przez inspektorów Biura Generalnego Inspektora Ochrony Danych Osobowych,

f) zgłaszanie skarg do Generalnego Inspektora Ochrony Danych Osobowych na niezgodne z ustawą przetwarzanie danych osobowych, które PIIB powierzył podmiotom trzecim,

g) udzielanie odpowiedzi na zapytania kierowane do PIIB przez podmioty zewnętrzne, dotyczące administrowanych zbiorów danych osobowych,

h) informowanie osób zgłaszających zastrzeżenia w związku z przetwarzaniem ich danych osobowych o legalności procesu przetwarzania danych – o podstawie prawnej, celu, zgodności systemów informatycznych przetwarzających dane z wymogami ustawy i rozporządzenia oraz wyznaczeniu ABI jako podmiotu czuwającego nad bezpieczeństwem danych osobowych.

Parafa:	

i) przeprowadzanie szkoleń z zakresu ochrony danych osobowych dla pracowników PIIB, którym mają być nadane upoważnienia do przetwarzania danych osobowych w trybie określonym w Rozdziale 3 niniejszej Polityki Bezpieczeństwa,

j) nadzór nad fizycznym zabezpieczeniem obszarów, w których przetwarzane są dane osobowe,

k) monitorowanie działania i skuteczności zabezpieczeń wdrożonych w celu ochrony danych osobowych,

l) opiniowanie w sprawie możliwości oraz prawidłowości zbierania danych osobowych w celu utworzenia zbioru danych osobowych, zbierania nowych kategorii danych do istniejącego już zbioru lub przetwarzania danych w innym celu niż ten, dla którego dane zostały zebrane,

m) opiniowanie w sprawie konieczności i stosowanej formie wykonywania obowiązku informacyjnego, o którym mowa w art. 24 i art. 25 Ustawy,

n) opiniowanie w sprawie udostępniania danych osobowych odbiorcom danych,

o) przygotowywanie lub opiniowanie umów dotyczących powierzenia przetwarzania danych osobowych lub decyzji w kwestii udostępnienia danych osobowych ze zbiorów,

p) wydawanie pisemnych zaleceń wszelkim osobom przetwarzającym dane osobowe celem przetwarzania ich zgodnie z Ustawą, Rozporządzeniem, Polityką Bezpieczeństwa oraz Instrukcją Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych,

q) kontrola przetwarzania i stanu zabezpieczenia danych osobowych przetwarzanych w PIIB,

r) inicjatywa i nadzór nad wdrażaniem w PIIB nowych rozwiązań w zakresie zabezpieczenia danych osobowych.

2.2.3. ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

1. Funkcję Administratora Systemów Informatycznych (ASI) pełni w PIIB Adam Kuśmierczyk.

2. Zmiana osoby pełniącej funkcję Administratora Systemów Informatycznych następuje na skutek pisemnej decyzji Administratora Danych - Krajowej Rady podpisanej przez Prezesa i sekretarza Krajowej Rady.

2. W przypadku odwołania lub rezygnacji ze stanowiska Administratora Systemów Informatycznych, Administrator Danych niezwłocznie wyznacza na to stanowisko inną osobę.

3. Do uprawnień i obowiązków Administratora Systemów Informatycznych należą, w szczególności:

   a) nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych,

   b) wnioskowanie do Dyrektora Krajowego Biura PIIB o konieczności nadania pracownikowi upoważnienia do przetwarzania danych osobowych w systemach informatycznych,

Parafa:	

c) nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,

d) podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,

e) identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych i tradycyjnych,

f) sprawowanie nadzoru nad przechowywanymi kopiami zapasowymi opisanymi w Instrukcji Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych,

g) inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych,

h) podejmowanie innych czynności w zakresie zabezpieczenia przetwarzania danych w systemach informatycznych, o których mowa w Instrukcji Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych,

i) informowanie Administratora Bezpieczeństwa Informacji o konieczności wprowadzenia zmian w Instrukcji Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych (z powodu np. zmian procedur tworzenia kopii zapasowych lub zmiany zabezpieczeń systemów informatycznych).

2.2.4. PRACOWNICY POLSKIEJ IZBY INŻYNIERÓW BUDOWNICTWA POSIADAJĄCY DOSTĘP DO DANYCH OSOBOWYCH

1. Każdy pracownik PIIB, który uzyskał upoważnienie do przetwarzania danych osobowych, zobowiązany jest do ich ochrony w sposób zgodny z przepisami Ustawy, Rozporządzenia, Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych.
2. Dostęp do określonego zbioru danych osobowych pracownik PIIB uzyskuje na podstawie pisemnego upoważnienia, otrzymanego w trybie określonym w Rozdziale 3, niniejszej Polityki Bezpieczeństwa.
3. Pracownicy zatrudnieni - na podstawie umowy o pracę, bądź świadczący usługi na podstawie umów cywilnoprawnych - przy przetwarzaniu danych osobowych zobowiązani są do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu

Parafa:	

zatrudnienia. Stosowny zapis o przyjęciu zobowiązania do zachowania w tajemnicy przetwarzanych danych osobowych zawiera upoważnienie, którego wzór znajduje się w Załączniku nr 4.

4. Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy skutkuje poniesieniem odpowiedzialności karnej na podstawie przepisów ustawy oraz stanowi ciężkie naruszenie obowiązków pracowniczych i może być podstawą rozwiązania stosunku pracy w trybie art. 52 Kodeksu Pracy.

3. UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. PIIB realizując niniejszą Politykę Bezpieczeństwa, w zakresie udostępniania danych osobowych w ramach własnej (wewnętrznej) struktury, zezwala na ich przetwarzanie w systemie informatycznym lub w wersji papierowej wyłącznie pracownikom, którzy uzyskali uprzednie, stosowne upoważnienie do przetwarzania danych osobowych, nadawane przez Dyrektora Krajowego Biura Polskiej Izby Inżynierów Budownictwa.
2. Upoważnienie do przetwarzania danych osobowych mogą uzyskać wyłącznie pracownicy PIIB.
3. Dostęp do danych osobowych i ich przetwarzania bez odrębnego upoważnienia, o którym mowa w niniejszym Rozdziale może mieć miejsce wyłącznie w przypadku działań podmiotów upoważnionych na mocy odpowiednich przepisów prawa.
   3.1 W szczególności dostęp do danych osobowych na podstawie zasady określonej w pkt. 3 posiadają: Państwowa Inspekcja Pracy, Zakład Ubezpieczeń Społecznych, organy skarbowe, Policja, Agencja Bezpieczeństwa Wewnętrznego, sądy powszechne, Najwyższa Izba Kontroli, Generalny Inspektor Ochrony Danych Osobowych, podmioty którym powierzono przetwarzanie danych osobowych oraz inne upoważnione przez przepisy prawa podmioty i organy, działające w granicach przyznanych im uprawnień – wszystkie w/w po okazaniu dokumentów potwierdzających te uprawnienia.
4. Upoważnienie, o którym mowa w niniejszym Rozdziale, wydawane jest każdemu z pracowników osobno, z wyraźnym wskazaniem, jakie zbiory danych obejmuje swoim zakresem.
5. Wzór upoważnienia stanowi Załącznik nr 4 do Polityki Bezpieczeństwa.
6. Upoważnienia w imieniu Administratora Danych nadaje Dyrektor Krajowego Biura Polskiej Izby Inżynierów Budownictwa, na mocy delegacji uprawnienia do nadawania upoważnień, nadanego przez Administratora Danych (stosowne upoważnienie znajduje się w Załączniku nr 3)
7. Upoważnienia wydawane są zgodnie z następującą procedurą:

7.1 Dział kadr lub Administrator Systemów Informatycznych bądź Administrator Bezpieczeństwa Informacji informują Dyrektora Krajowego Biura PIIB o konieczności nadania pracownikowi upoważnienia do przetwarzania danych osobowych w określonych zbiorach.

7.2 Administrator Bezpieczeństwa Informacji przed nadaniem pracownikowi upoważnienia, organizuje dla niego krótkie szkolenie, podczas którego osoba jest informowana o podstawowych aspektach prawnych związanych z ochroną danych osobowych (najważniejsze definicje, odpowiedzialność prawna, obowiązek właściwego zabezpieczenia danych przetwarzanych w formie papierowej oraz w systemach informatycznych). Szkolenie może zostać przeprowadzone w następującej formie:

7.2.1 osobiście przez Administratora Bezpieczeństwa Informacji bądź wyznaczoną przez niego osobę w siedzibie PIIB,

7.2.2 w formie e-learningu za pośrednictwem internetowej platformy szkoleniowej. Pracownik po otrzymaniu loginu i hasła do platformy uczestniczy w szkoleniu samodzielnie. Szkolenie zostanie zakończone w momencie, kiedy wiedza pracownika z zakresu ochrony danych osobowych zostanie zweryfikowana pomyślnie za pomocą testu.

7.3 Dyrektor Krajowego Biura PIIB sporządza upoważnienie dla pracownika, który wykaże, że odbył i pomyślnie ukończył szkolenie.

7.4 Poza szkoleniem, którego odbycie warunkuje uzyskanie uprawnień do nadania pracownikowi upoważnienia do przetwarzania danych osobowych, dodatkowo będą odbywały się cykliczne szkolenia dotyczące doskonalenia i utrwalania wiedzy z zakresu ochrony danych osobowych dla pracowników PIIB, w formie i terminach ustalonych przez Administratora Bezpieczeństwa Informacji.

7.5 Upoważnienie jest drukowane w dwóch egzemplarzach, z których każdy musi być podpisany przez pracownika któremu nadano upoważnienie.

7.6 Jeden egzemplarz upoważnienia jest przechowywany jako część dokumentacji kadrowej, drugi jest wydawany pracownikowi któremu nadano upoważnienie.

7.7 Wydanie każdego upoważnienia jest odnotowywane przez Dyrektora Krajowego Biura PIIB w prowadzonej i nadzorowanej przez niego elektronicznej ewidencji upoważnień we wszystkich zbiorach danych osobowych oraz przez dział kadr w papierowej ewidencji upoważnień która stanowi Załącznik nr 5 do niniejszej Polityki Bezpieczeństwa.

8. W przypadku stwierdzenia, iż dany pracownik uzyskał zbyt szerokie uprawnienia w zakresie przetwarzania danych osobowych, nieuzasadnione wykonywanymi przez niego zadaniami służbowymi lub innymi obowiązkami o charakterze merytorycznym, oraz gdy było to przyczyną naruszenia poziomu bezpieczeństwa przetwarzania danych osobowych uznaje się, iż odpowiedzialność służbową za to ponosi

Parafa:	

Administrator Bezpieczeństwa Informacji. Podobny zakres odpowiedzialności spoczywa na Administratorze Bezpieczeństwa Informacji w przypadku uchybienia innym wymogom dotyczącym dopuszczenia do przetwarzania danych osobowych przewidzianym w niniejszym Rozdziale.

9. Zakres nadanych pracownikowi uprawnień może ulegać zmianie (rozszerzeniu bądź zawężeniu) w związku z pełnieniem przez niego określonych zadań w określonym przedziale czasu. W takim przypadku tryb wskazany do nadawania uprawnień określony w przedmiotowym Rozdziale jest właściwy również w razie zmiany zakresu uprawnień pracownika w związku z jego dostępem do określonego zbioru danych osobowych.
10. W przypadku zaistnienia konieczności cofnięcia upoważnienia do przetwarzania danych osobowych, informuje się o tym Dyrektora Krajowego Biura PIIB oraz dział kadr w celu aktualizacji ewidencji upoważnień.
11. Utrata prawa do przetwarzania danych osobowych określonych w upoważnieniu następuje w szczególności w przypadku:
    - 11.1 zmiany stanowiska pracy w PIIB na stanowisko, na którym nie ma konieczności posiadania dostępu do danych osobowych lub w szczególności, gdy ustaje zasadność i celowość dalszego wykonywania prawa do przetwarzania danych w związku ze zmianą realizowanych przez pracownika zadań wynikających z jego indywidualnego zakresu czynności,
    - 11.2 umyślnego naruszenia zasad ochrony danych osobowych określonych w Ustawie, Rozporządzeniu, Polityce Bezpieczeństwa, Instrukcji Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych,
    - 11.3 rozwiązania stosunku pracy,
    - 11.4 rozwiązania umowy cywilnoprawnej,
    - 11.5 aktualizacji wzoru upoważnienia. W takim przypadku wszystkim pracownikom którzy byli do tej pory upoważnieni do przetwarzania danych osobowych, niezwłocznie wydawane są nowe upoważnienia zgodnie z procedurą opisaną w pkt. 7 niniejszego Rozdziału.
12. Uszczegółowienie trybu nadania, zmiany, utraty uprawnień logicznego dostępu do danych osobowych przetwarzanych w systemach informatycznych zawiera Instrukcja Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych.

4. INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Osobą odpowiedzialną za bezpieczeństwo danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do pomieszczeń oraz systemów, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń, jest Administrator Bezpieczeństwa Informacji.
2. Za naruszenie ochrony danych osobowych uważa się w szczególności:
   2.1 nieuprawniony dostęp lub próbę dostępu do systemu lub pomieszczeń w których następuje proces przetwarzania danych (widoczne uszkodzenia bądź naruszenia zabezpieczeń);
   2.2 naruszenie lub próbę naruszenia zbioru danych oraz integralności systemu;
   2.3 nieautoryzowane zniszczenie lub próbę zniszczenia danych zgromadzonych w zbiorach papierowych oraz systemie;
   2.4 zmianę lub utratę danych zapisanych na kopiach zapasowych lub archiwalnych dokonaną w sposób nieautoryzowany; nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu);
   2.5 inny stan systemu lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu lub po przerwie w pracy z systemem.
2. Instrukcję stosuje się odpowiednio w przypadku stwierdzenia, że stan dokumentacji lub stan pomieszczeń bądź szaf biurowych, w których przechowywana jest dokumentacja wzbudzają podejrzenie, że dostęp do nich mogły mieć osoby nieupoważnione.
3. W przypadku stwierdzenia naruszenia danych w systemie informatycznym lub zaistnienia okoliczności wskazujących na naruszenie zabezpieczeń systemu informatycznego, w którym przetwarzane są dane osobowe, użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie Administratora Bezpieczeństwa Informacji.
4. Do czasu przybycia Administratora Bezpieczeństwa Informacji, użytkownik:

Parafa:	

4.1 zabezpiecza dostęp do miejsca lub urządzenia;

4.2 wstrzymuje pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamia bez koniecznej potrzeby komputerów i innych urządzeń, które w związku z naruszeniem ochrony zostały wstrzymane;

4.3 podejmuje, stosownie do zaistniałej sytuacji inne, niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

5. Administrator Bezpieczeństwa Informacji po przybyciu na miejsce, w którym doszło do naruszenia ochrony danych osobowych:

5.1 ocenia zaistniałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane osobowe, stan urządzeń i zbioru danych;

5.2 podejmuje niezbędne działania mające na celu uniemożliwienie dalszego naruszenia zabezpieczenia systemu (odłączenie urządzeń, odłączenie wadliwych urządzeń, zmiana haseł, blokowanie dostępu do sieci telekomunikacyjnej, programów oraz zbiorów danych);

5.3 zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia, jak również sprawdza zawartość zbioru danych osobowych;

5.4 sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych;

5.5 sprawdza sposób działania programu (w tym również obecność wirusów komputerowych);

5.6 ustala charakter i rodzaj naruszenia oraz metody działania osób naruszających zabezpieczenie systemu;

5.7 niezwłocznie zapewnia przywrócenie prawidłowego stanu działania systemu, a w przypadku uszkodzenia baz danych, odtwarza je z ostatnich kopii awaryjnych z zachowaniem należytych środków ostrożności;

5.8 sprawdza jakość komunikacji w systemie informatycznym;

5.9 dokonuje analizy stanu systemu wraz z oszacowaniem rozmiaru szkód powstałych wskutek naruszenia oraz poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych;

5.10 spisuje relację osoby zatrudnionej przy przetwarzaniu danych, która dokonała powiadomienia;

5.11 podejmuje decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych i w przypadkach uzasadnionych niezwłocznie powiadamia Dyrektora Krajowego Biura Polskiej Izby Inżynierów Budownictwa;

5.12 sporządza szczegółowy raport zawierający w szczególności: dane personalne osoby, która stwierdziła naruszenie, datę i godzinę powiadomienia, opis podjętych czynności i ich uzasadnienie.

6. Raport, o którym mowa w ust. 3 pkt 12 przekazywany jest bezzwłocznie Dyrektorowi Krajowego Biura Polskiej Izby Inżynierów Budownictwa.

7. Zgodę na ponowne uruchomienie komputerów i innych urządzeń oraz kontynuowanie pracy wyraża Administrator Bezpieczeństwa Informacji.

Parafa:	

8. Dokonywanie zmian w miejscu naruszenia ochrony bez uzyskania zgody, o której mowa w ust. 5 jest dopuszczalne, jeżeli zachodzi konieczność ratowania osób lub mienia albo zapobieżenia grożącemu niebezpieczeństwu.
9. Administrator Bezpieczeństwa Informacji podejmuje niezbędne działania w celu wyeliminowania naruszeń zabezpieczeń danych w przyszłości, a w szczególności:
   9.1 jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego lub jakość komunikacji w sieci telekomunikacyjnej, niezwłocznie przeprowadza, w stosownym zakresie, przeglądy oraz konserwacje urządzeń i programów, ustala źródło pochodzenia wirusa oraz wdraża skuteczniejsze zabezpieczenia antywirusowe, a w miarę potrzeby kontaktuje się z dostawcę usług telekomunikacyjnych;
   9.2 jeżeli przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, przeprowadza dodatkowe kursy i szkolenia osób biorących udział przy przetwarzaniu danych, a wobec osób winnych zaniedbań wnioskuje o ich ukaranie w trybie przewidzianym odrębnymi przepisami.

Parafa:	

5. UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

1. PIIB realizując niniejszą Politykę Bezpieczeństwa dopuszcza, by dane osobowe których jest administratorem, były przetwarzane poza własnymi strukturami organizacyjnymi. Może się to odbywać wyłącznie na drodze powierzenia danego zbioru w określonym celu i zakresie podmiotowi zewnętrznemu na mocy umowy powierzenia przetwarzania danych osobowych.
2. Pisemna umowa powierzenia przetwarzania danych osobowych, o której mowa w niniejszym Rozdziale musi być zgodna z postanowieniami art. 31 ustawy o ochronie danych osobowych.
3. Powierzenia przetwarzania danych osobowych zgodnie z przepisami ustawy o samorządach zawodowych architektów, inżynierów budownictwa oraz urbanistów oraz Regulaminem Krajowej Rady PIIB można dokonać: na podstawie oświadczenia woli w formie decyzji Krajowej Rady PIIB podjętej i podpisanej przez Prezesa i Sekretarza Krajowej Rady Biura PIIB. Powierzenie przetwarzania danych osobowych może nastąpić na podstawie pisemnej umowy, aneksu do umowy lub klauzuli do umowy.
4. W przypadku, gdy powierzenie danych osobowych wynika wprost z zawartej z danym podmiotem umowy, nie ma konieczności sporządzania dodatkowo pisemnej umowy powierzenia danych osobowych.
5. Każdorazowe dokonanie powierzenia danych osobowych o którym mowa w niniejszym Rozdziale musi obligatoryjnie zostać odnotowane w Polityce Bezpieczeństwa.
6. PIIB w zakresie prowadzonej przez siebie działalności może przetwarzać również dane osobowe powierzone jej przez swoich klientów, na rzecz których świadczy swe usługi. Administratorem powyższych danych są poszczególni klienci PIIB, którzy obowiązani są do zawarcia pisemnej umowy powierzenia przetwarzania w/w danych.
7. Każdorazowo informuję się Administratora Bezpieczeństwa Informacji o zawarciu umowy powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu.

6. WYKAZ ZBIORÓW DANYCH WRAZ ZE WSKAZANIEM PROGRAMÓW STOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

Nr	NAZWA ZBIORU DANYCH	SYSTEMY INFORMATYCZNE STOSOWANE DO PRZETWARZANIA DANYCH OSOBOWYCH W ZBIORZE	UWAGI
1.	Rejestr Członków PIIB w tym rejestr członków ukaranych	BUDINFO	Dane osobowe członków PIIB przetwarzane w związku członkostwem w PIIB w tym także w związku z prowadzeniem postępowania w sprawach odpowiedzialności zawodowej w budownictwie, prowadzeniem postępowania dyscyplinarnego.
2.	Rejestr potencjalnych członków PIIB	BUDINFO	Dane osobowe osób z nowo nadanymi uprawnieniami budowlanymi/ nowo nadanym tytułem rzeczoznawcy budowlanego przetwarzane w celu uzyskania członkostwa.
3.	Rejestr rzeczoznawców	BUDINFO	Dane osobowe członków PIIB, którym nadano tytuł rzeczoznawcy budowlanego.
4.	Rejestr egzaminacyjny	BUDINFO	Dane osobowe osób ubiegających się o nadanie uprawnień budowlanych/ tytułu rzeczoznawcy budowlanego.
5.	Rejestr kadrowy Krajowego Biura PIIB	SYMFONIA KADRY I PŁACE	Dane osobowe pracowników Krajowego Biura PIIB przetwarzane w związku z zatrudnieniem.
6.	Rejestr promujący aktywność zawodową członków PIIB	BRAK	Dane osobowe członków przetwarzane w związku z funkcjonowaniem internetowej wyszukiwarki ankiety zawodowej członków PIIB.

Parafa:	

7. OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ PÓL INFORMACYJNYCH I POWIĄZANIA MIĘDZY POSZCZEGÓLNYMI POLAMI INFORMACYJNYMI

Nr	NAZWA ZBIORU DANYCH	ZAKRES PRZETWARZANYCH DANYCH
1.	Rejestr Członków PIIB	Imię i nazwisko, data urodzenia, PESEL, nazwisko rodowe, obywatelstwo, tytuł naukowy, adres zamieszkania, adres korespondencyjny, numer telefonu, adres e-mail, adres do wysyłki czasopism, numer członkowski, miejsce pracy. Uprawnienia budowlane – numer, data wydania, specjalność, specjalizacja, przez kogo zostały wydane. Informacje o składkach na ubezpieczenie, informacje o zawieszeniu, skreśleniu z listy członków, informacje o odbytych szkoleniach w PIIB, informacje o zapomogach. Znajomość języków obcych. Informacje o nałożonych karach.
2.	Rejestr potencjalnych członków PIIB	Imię i nazwisko, imię ojca, data urodzenia, PESEL, miejsce urodzenia, nazwisko rodowe, obywatelstwo, adres zamieszkania, adres do korespondencji, numer telefonu, numer fax., adres e-mail. Tytuł, numer ewidencyjny uprawnień budowlanych, data wydania, specjalność. Znajomość języków obcych.
3.	Rejestr rzeczoznawców	Imię i nazwisko, imię ojca, data urodzenia, PESEL, miejsce urodzenia, nazwisko rodowe, obywatelstwo, adres zamieszkania, adres do korespondencji, numer telefonu, numer fax., adres e-mail, numer członkowski. Sygnatura akt, tytuł, numer ewidencyjny uprawnień budowlanych, data wydania, specjalność. Znajomość języków obcych.
4.	Rejestr egzaminacyjny	Imię nazwisko, adres, numer telefonu, data urodzenia i miejsce urodzenia, PESEL, nr paszportu lub innego dokumentu potwierdzającego tożsamość gdy osoba nie posiada obywatelstwa polskiego, wykształcenie, tytuł naukowy/zawodowy, zakład pracy w którym odbywana była praktyka zawodowa oraz stanowisko. Posiadane uprawnienia budowlane.
5.	Rejestr kadrowy Krajowego Biura PIIB	Imię/imiona, nazwisko, nazwisko rodowe, NIP, PESEL, data urodzenia, miejsce urodzenia, numer dowodu osobistego lub paszportu, informacje o organie który wydał dokument, telefon, adres zamieszkania (adres stały, adres tymczasowy), adres do korespondencji, data rozpoczęcia/zwolnienia z pracy, numer ewidencyjny pracownika, imię ojca, imię matki. Stopień pokrewieństwa pracownika w stosunku do pracodawcy.
6.	Rejestr promujący aktywność zawodową członków PIIB	Imię, nazwisko, powiat, miejscowość, wykonywany zawód, specjalność zawodowa, znajomość języków.

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi zawiera Załącznik nr 6 do niniejszej Polityki.

Parafa:	

8. SPOSÓB PRZEPŁYWU DANYCH OSOBOWYCH POMIĘDZY SYSTEMAMI INFORMATYCZNYMI

Pomiędzy systemami BUDINFO oraz SYMFONIA KADRY I PŁACE nie występuje eksport danych.

Parafa:	

9. WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

	ADRES / LOKALIZACJA	UWAGI
Dane osobowe przetwarzane jako Administrator Danych	**POLSKA IZBA INŻYNIERÓW BUDOWNICTWA** ul. Mazowiecka 6/8 00-048 Warszawa	
Dane osobowe powierzone do przetwarzania Przetwarzającemu (na podstawie umowy powierzenia przetwarzania danych osobowych)	**POCZTA POLSKA SPÓŁKA AKCYJNA,** ul. Rakowiecka 26, 00- 940 Warszawa	Stała współpraca polegająca przetwarzaniu danych osobowych w celu: 1. przygotowania i wykonania wysyłki czasopisma „Inżynier Budownictwa" wraz z innymi materiałami przekazywanymi do członków PIIB. 2. wysyłki druków opłat na rzecz Nadawcy.
	SOFTEX DATA S.A., ul. Poleczki 47, 02-822 Warszawa	Usługi w zakresie przetwarzania danych osobowych w związku z dokonywaniem wydruków, personalizacją, insertowaniem i nadawaniem korespondencji masowej.
	ENTIM ul. Targowa 80/82 lok. 15, 03-448 Warszawa	Usługi w zakresie przetwarzania danych osobowych w zakresie zbierania tych danych i wstępnego przetwarzania w systemie informatycznym i przekazania opracowanych baz do firm SOFTEX DATA i CER Poczta Polska.

Parafa:	

	ENTIM ul. Targowa 80/82 lok. 15, 03-448 Warszawa	Usługa związana z kompleksowym wsparciem technicznym i doradczym oraz zarządzaniem architekturą systemu BUDINFO w PIIB.
	INONE SPÓŁKA AKCYJNA ul. Łąkowa 29 90-554 Łódź	Usługa przetwarzania danych osobowych w zakresie ich przechowywania wyłącznie w celu związanym z wykonywaniem umowy dzierżawy
Dane osobowe udostępnione PIIB oraz dane, które PIIB udostępnia	**Ubezpieczenia STU Ergo Hestia S.A.** ul. Sienkiewicza 11, 44-100 Gliwice	Udostępnianie danych wiąże się z realizacją zawartej umowy.
	Dolnośląska Okręgowa Izba Inżynierów Budownictwa, ul. Odrzańska 22, 50-114 Wrocław	Współpraca polega na realizacji przez poszczególne jednostki organizacyjne PIIB obowiązków wynikających z przepisów prawa oraz spełniania wynikających z nich uprawnień.
	Kujawsko-Pomorska Okręgowa Izba Inżynierów Budownictwa, ul. Rumińskiego 6, 85-030 Bydgoszcz	
	Lubelska Okręgowa Izba Inżynierów Budownictwa, ul. Bursaki 19, 20-150 Lublin	
	Lubuska Okręgowa Izba Inżynierów Budownictwa, Gorzów Wlkp. ul. Kazimierza Wielkiego 10,	

Parafa:	

	66-400 Gorzów Wlkp.	
	Łódzka Okręgowa Izba Inżynierów Budownictwa, ul. Północna 39, 91-425 Łódź	
	Małopolska Okręgowa Izba Inżynierów Budownictwa, ul. Czarnowiejska 80, 30-054 Kraków	
	Mazowiecka Okręgowa Izba Inżynierów Budownictwa, ul. 1 Sierpnia 36 B, 02-134 Warszawa	
	Opolska Okręgowa Izba Inżynierów Budownictwa, ul. Katowicka 50, 45- 061 Opole	
	Podkarpacka Okręgowa Izba Inżynierów Budownictwa, ul. Słowackiego 20, 35-060 Rzeszów	
	Podlaska Okręgowa Izba Inżynierów Budownictwa, ul. Legionowa 28 Lok. 402, 15-281 Białystok	
	Pomorska Okręgowa Izba Inżynierów Budownictwa, ul. Świętojańska 43/44, 80-840 Gdańsk	

Parafa:	

	Śląska Okręgowa Izba Inżynierów Budownictwa, ul. Podgórna 4, 40-026 Katowice	
	Świętokrzyska Okręgowa Izba Inżynierów Budownictwa, ul. Św. Leonarda 18, 25-304 Kielce	
	Warmińsko-Mazurska Okręgowa Izba Inżynierów Budownictwa, Plac Konsulatu Polskiego 1, 10-532 Olsztyn	
	Wielkopolska Okręgowa Izba Inżynierów Budownictwa, ul. Dworkowa 14, 60-602 Poznań	
	Zachodniopomorska Okręgowa Izba Inżynierów Budownictwa, ul. Energetyków 9, 70-656 Szczecin	

Parafa:	

10. ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH

10.2. ŚRODKI TECHNICZNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH

Środek techniczny	Uwagi
Dostęp do pomieszczeń, w których przetwarzany jest zbiory danych osobowych objęte są systemem kontroli dostępu.	Na portierni prowadzony jest rejestr osób, którym wydawane sa klucze.
Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi).	
Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych.	

Parafa:	

Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony.	
Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych przez cała dobę jest nadzorowany przez służbę ochrony.	
Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętym pomieszczeniu zabezpieczonymi drzwiami o podwyższonej wytrzymałości.	Dotyczy danych gromadzonych w archiwum.
Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej metalowej szafie.	[redacted]
Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.	
Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.	

10.3. ŚRODKI ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH

Środek organizacyjny	Uwagi
Do przetwarzania danych osobowych dopuszczono wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.	

Parafa:	

Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.	
Wyznaczono Administratora Bezpieczeństwa Informacji.	Funkcję Administratora Bezpieczeństwa Informacji pełni Adam Kuśmierczyk
Wyznaczono Administratora Systemów Informatycznych.	Funkcję Administratora Systemów Informatycznych pełni Adam Kuśmierczyk
Opracowano i wdrożono Politykę Bezpieczeństwa o której mowa w ustawie o ochronie danych osobowych.	
Opracowano i wdrożono Instrukcję Zarządzania Systemem Informatycznym służącymi do przetwarzania danych osobowych.	
Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.	
Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.	
Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy.	
Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym.	

Parafa:	

Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.	

11. ZAŁĄCZNIKI

Załącznik nr 1 – Ustanowienie Administratora Bezpieczeństwa Informacji.

Załącznik nr 2 - Ustanowienie Administratora Systemów Informatycznych.

Załącznik nr 3 -Delegacja uprawnienia do nadawania upoważnień do przetwarzania danych osobowych.

Załącznik nr 4 - Wzór upoważnienia do przetwarzania danych osobowych.

Załącznik nr 5 – Ewidencja osób upoważnionych do przetwarzania danych osobowych.

Załącznik nr 6 - Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.

Parafa:	

Dokument sporządzono:	**Pełen podpis Administratora Danych:**	**Pieczęć**
Data: __/__/____(dd/mm/rrrr) Miejsce:		

Parafa:	

Załącznik nr 1- Ustanowienie Administratora Bezpieczeństwa Informacji

Niniejszym, zgodnie z dyspozycją Rozdziału 3 Polityki Bezpieczeństwa oraz reprezentując Administratora Danych – Polską Izbę Inżynierów Budownictwa z siedzibą przy ul. Mazowieckiej 6/8, 00-048 w Warszawie,

wyznaczamy

Pana Adama Kuśmierczyka na stanowisko Administratora Bezpieczeństwa Informacji (ABI) w Polskiej Izbie Inżynierów Budownictwa.

Zakres pozostałych obowiązków oraz warunki pełnienia funkcji Administratora Bezpieczeństwa Informacji określone są ustawą o ochronie danych osobowych z dnia 29 sierpnia 1997 roku oraz dokumentacją z zakresu ochrony danych osobowych wdrożoną dnia 1 / 03 / 2012 r. (dd/mm/rrrr) w Polskiej Izbie Inżynierów Budownictwa.

PODPISY:

Parafa:	

Załącznik nr 2- Ustanowienie Administratora Systemów Informatycznych

Niniejszym, zgodnie z dyspozycją Rozdziału 3 Polityki Bezpieczeństwa oraz reprezentując Administratora Danych – Polską Izbę Inżynierów Budownictwa z siedzibą przy ul. Mazowieckiej 6/8, 00-048 w Warszawie

wyznaczam

Pana Adama Kuśmierczyka na stanowisko Administratora Systemów Informatycznych (ASI) w Polskiej Izbie Inżynierów Budownictwa.

Zakres obowiązków oraz warunki pełnienia funkcji Administratora Systemów Informatycznych określone są w dokumentacji z zakresu ochrony danych osobowych wdrożonej dnia 1 / 03 / 2012 r. (dd/mm/rrrr) w Polskiej Izbie Inżynierów Budownictwa.

PODPIS:

Parafa:	

Załącznik nr 3 – Delegacja uprawnienia do nadawania upoważnień do przetwarzania danych osobowych

Niniejszym zgodnie z dyspozycją Rozdziału 3 Polityki Bezpieczeństwa oraz reprezentując Administratora Danych – Polską Izbę Inżynierów Budownictwa z siedzibą przy ul. Mazowieckiej 6/8, 00-048 w Warszawie,

upoważniam

Dyrektora Krajowego Biura Polskiej Izby Inżynierów Budownictwa Andrzeja Orczykowskiego do nadawania w imieniu administratora danych upoważnień do przetwarzania danych osobowych.

PODPIS:

Parafa:	

Załącznik nr 4 – Wzór upoważnienia do przetwarzania danych osobowych

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym jako Dyrektor Krajowego Biura Polskiej Izby Inżynierów Budownictwa, reprezentując Administratora Danych – Polską Izbę Inżynierów Budownictwa z siedzibą przy ul. Mazowieckiej 6/8, 00-048 w Warszawie, na mocy stosownego umocowania nadanego na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002 r., Nr 101, poz. 926 z późn. zm.),

upoważniam

do przetwarzania danych osobowych Pana/Panią (dalej: osoba upoważniona):

Imię i nazwisko	

Przedmiotowe upoważnienie obejmuje swoim zakresem następujące zbiory danych osobowych:

Nr	**Nazwa zbioru danych osobowych**	**Zakres** (wgląd, wprowadzania, przechowywania, modyfikacji, usuwania itp.)	**Wersja zbioru** -zbiór w systemie informatycznym - zbiór w wersji papierowej
1			
2			
3			
4			
5			
6			

Parafa:	

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w w/w zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem administratora danych.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002 r., Nr 101, poz. 926 z późn. zm.), wydanych na jej podstawie aktów wykonawczych i obowiązujących w PIIB wewnętrznych regulacji w sprawie ochrony danych osobowych.

Naruszenie w/w obowiązków może skutkować poniesieniem odpowiedzialności karnej, na podstawie przepisów określonych w ustawie o ochronie danych osobowych oraz stanowi ciężkie naruszenie obowiązków pracowniczych, które może być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu Pracy.
Upoważnienie jest ważne do odwołania.

…… Data i podpis osoby upoważnionej do przetwarzania danych osobowych	…… Data i podpis upoważniającego.

Oświadczenie

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w PIIB (w szczególności z Polityką Bezpieczeństwa oraz Instrukcją Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych). Przyjmuję do wiadomości zawarte w nich obowiązki w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych na zajmowanym stanowisku i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu zatrudnienia.

……..……..

Data i podpis pracownika

Rozdzielnik 2 egz. w oryginale:
1 x oryginał dział kadr
1 x oryginał pracownik uzyskujący upoważnienie

Parafa:	

Załącznik nr 5 – Ewidencja osób upoważnionych do przetwarzania danych osobowych

Nr	Imię i nazwisko osoby upoważnionej	Data nadania upoważnienia	Data ustania upoważnienia	Indywidualny identyfikator w systemie informatycznym	Nazwy zbiorów objętych zakresem upoważnienia
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					
16.					
17.					
18.					
19.					

Parafa:	

21.					
22.					
23.					
24.					
25.					
26.					
27.					
28.					
29.					
30.					

Dokument sporządzono:	**Pełen podpis Dyrektora Krajowego Biura PIIB**	**Pieczęć**
Data: __/__/____(dd/mm/rrrr) Miejsce:		

Parafa:	

Parafa:	