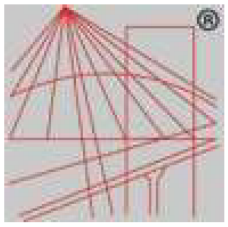

POLSKA IZBA INŻYNIERÓW BUDOWNICTWA

POLSKA IZBA INŻYNIERÓW BUDOWNICTWA

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

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Data i miejsce sporządzenia dokumentu:	1 / 03 / 2012 r. (dd/mm/rrrr)
Ilość stron:	23
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:	

Parafa:	

1. WSTĘP

1.1. INFORMACJE OGÓLNE

Niniejszy dokument w postaci Instrukcji Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych został opracowany przez Administratora Danych – Polską Izbę Inżynierów Budownictwa w celu zapewnienia zgodności przetwarzania danych osobowych z polskim prawem.

Instrukcja Zarządzania Systemem Informatycznym wraz z Polityką Bezpieczeństwa 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.).

Instrukcja Zarządzania Systemem Informatycznym obowiązuje od dnia 1 / 03 / 2012 r. (dd/mm/rrrr). Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów niniejszego dokumentu Instrukcji Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych, 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 na podstawie upoważnienia Administratora Danych, została zapoznana z Instrukcją Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych i zobowiązana do jej przestrzegania w zakresie wynikającym z przydzielonych zadań. Dotyczy to w szczególności pracowników zatrudnionych przez Administratora Danych. Wyżej wymienione osoby złożyły na piśmie oświadczenie o zapoznaniu się z treścią Instrukcji Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych oraz zobowiązały się do stosowania zawartych w niej postanowień.

Najniższa Instrukcja Zarządzania Systemem Informatycznym wraz z Polityką Bezpieczeństwa dotyczy Krajowej Izby Inżynierów Budownictwa

1.2. CEL PRZYGOTOWANIA INSTRUKCJI ZARZĄDZANIA

Podstawowym celem przyświecającym przygotowaniu i wdrożeniu dokumentu Instrukcji Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych było zapewnienie zgodności działania Polskiej Izby Inżynierów Budownictwa z ustawą o ochronie danych osobowych oraz z jej rozporządzeniami wykonawczymi. Dokument Instrukcji Zarządzania Systemem Informatycznym został opracowany na podstawie następujących aktów 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 Instrukcji Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych 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 INSTRUKCJĄ ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Dokument Instrukcji Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem. Obejmuje on ogólne informacje o systemie informatycznym i zbiorach danych osobowych, które są przy ich użyciu przetwarzane, o zastosowanych rozwiązaniach technicznych, jak również o procedurach eksploatacji i zasady użytkowania, jakie zastosowano w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych. Na Instrukcję Zarządzania składają się w szczególności następujące informacje:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
5) sposób, miejsce oraz okres przechowywania:
    a) elektronicznych nośników informacji zawierających dane osobowe,
    b) kopii zapasowych, o których mowa w pkt 4,
6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia;
7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia;
8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Instrukcję Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych 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, stosuje się zasady przetwarzania danych osobowych ujęte w niniejszym dokumencie Instrukcji Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych. Rygorowi Instrukcji Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych podlegają także dane powierzone Polską Izbę 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 INSTRUKCJI ZARZĄDZANIA

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. z 2002 r. Nr 101, poz. 926 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 **Instrukcji Zarządzania Systemem Informatycznym** 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** Służącym do przetwarzania danych osobowych – 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,

Parafa:	

10) **państwo trzecie** – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego,
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) **usuwanie 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. PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMACH INFORMATYCZNYCH ORAZ WSKAZANIA OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI

2.1. PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMACH INFORMATYCZNYCH

1. Uprawnienia do przetwarzania danych osobowych w systemach informatycznych nadaje każdorazowo Administrator Systemów Informatycznych.
2. W celu nadania uprawnienia o którym mowa w pkt 1, lub zmiany jego zakresu właściwy kierownik działu organizacyjnej Polskiej Izby Inżynierów Budownictwa lub zainteresowany pracownik występuje z umotywowanym wnioskiem do Administratora Systemów Informatycznych.
3. Uprawnienie do przetwarzania danych osobowych w systemach informatycznych może zostać nadane wyłącznie pracownikom, którzy uzyskali upoważnienie do przetwarzania danych osobowych nadane przez Dyrektora Krajowego Biura PIIB.
    3.1. Administrator Systemów Informatycznych każdorazowo decyduje czy istnieje konieczność (w celu wykonywania obowiązków zawodowych) nadania upoważnionemu pracownikowi uprawnienia do przetwarzania danych osobowych w systemach informatycznych.
    3.2. Zakres uprawnienia (zakres dostępu do danych osobowych przetwarzanych w systemach informatycznych) nie może być szerszy niż w wydanym wcześniej upoważnieniu.
4. Przydzielanie poszczególnym pracownikom Polskiej Izby Inżynierów Budownictwa uprawnień do przetwarzania danych osobowych w systemach informatycznych następuje poprzez nadanie im loginu oraz hasła tymczasowego pozwalającego na dostęp do danego systemu informatycznego (zgodnie z trybem określonym w Rozdziale 3 pkt. 1-7 niniejszej Instrukcji).
5. Administrator Systemów Informatycznych prowadzi rejestr nadanych uprawnień do przetwarzania danych w systemach informatycznych.
6. Jeśli Administrator Systemów Informatycznych uzna to za stosowne, uprawnienie dostępu do danego systemu informatycznego może zostać w każdej chwili cofnięte poprzez ograniczenie/ uniemożliwienie dostępu do przetwarzania danych z systemach informatycznych.

Parafa:	

7. Cofnięcie uprawnienia dostępu do danego systemu informatycznego Administrator Systemów Informatycznych odnotowuje w prowadzonym przez siebie w rejestrze nadanych uprawnień

Parafa:	

2.2. OSOBY ODPOWIEDZIALNE ZA NADAWANIE UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMACH INFORMATYCZNYCH

Zakres odpowiedzialności	Imię i nazwisko osoby odpowiedzialnej	Pełniona funkcja / uwagi
Przegląd przestrzegania Instrukcji	Adam Kuśmierczyk	Administrator Systemów Informatycznych
Przegląd aktualności Instrukcji	Adam Kuśmierczyk	Administrator Systemów Informatycznych
Nadawanie uprawnień do przetwarzania danych w systemach informatycznych	Adam Kuśmierczyk	Administrator Systemów Informatycznych
Rejestrowanie uprawnień do przetwarzania danych w systemach informatycznych	Adam Kuśmierczyk	Administrator Systemów Informatycznych
Wyrejestrowanie uprawnień do przetwarzania danych w systemach informatycznych	Adam Kuśmierczyk	Administrator Systemów Informatycznych

Parafa:	

3. OPIS STOSOWANYCH METOD I ŚRODKÓW UWIERZYTELNIENIA ORAZ PROCEDUR ZWIĄZANYCH Z ZARZĄDZANIEM I UŻYTKOWANIEM STOSOWANYCH METOD I ŚRODKÓW UWIERZYTELNIENIA

1. Dla każdego upoważnionego użytkownika systemu informatycznego ustala się odrębne konto zawierające w szczególności: identyfikator, hasło pierwszego logowania, dane o uprawnieniach użytkownika, profil.
2. Hasła tymczasowe do konta użytkownika (w przypadku utworzenia nowego konta, a także w sytuacjach awaryjnych związanych np.: z zagubieniem, utratą lub zapomnieniem hasła osobistego przez użytkownika konta) tworzone są przez Administratora Systemów Informatycznych.
3. Tryb przekazywania w/w hasła tymczasowego odbywa się za pośrednictwem poczty elektronicznej, w sposób zapewniający bezpieczeństwo i poufność przekazywanych informacji, w szczególności: w sposób uniemożliwiający innej osobie ich podsłuchanie lub nieuprawnione wykorzystanie.
4. Zezwala się na wykorzystanie innych, niewymienionych w Rozdziale 3 pkt. 3 niniejszej Instrukcji, bezpiecznych metod i środków technicznych, w celu przekazania hasła tymczasowego, za pisemną zgodą Administratora Systemów Informatycznych.
5. Zakazuje się przekazywania haseł tymczasowych poprzez osoby trzecie lub przy użyciu metod, które nie gwarantują zachowania jego poufności oraz niezaprzeczalnego ustalenia nadawcy i odbiorcy hasła, np.: przez niechronione wiadomości przekazywane elektronicznie.
6. Po otrzymaniu hasła tymczasowego użytkownik ma obowiązek niezwłocznego zalogowania się do systemu informatycznego przy użyciu tego hasła oraz jego zmiany na hasło osobiste.
7. Ujawnianie przez użytkownika komukolwiek, jakichkolwiek aktualnych lub poprzednich haseł tymczasowych, haseł osobistych lub innych haseł mu powierzonych, jest zabronione.
8. Autoryzacja do wszystkich programów przetwarzających dane osobowe, opisanych w niniejszej Instrukcji możliwa jest wyłącznie za pomocą loginu i hasła.
9. Jeżeli do uwierzytelniania użytkowników używa się hasła, jego zmiana musi następować nie rzadziej niż co 30 dni, hasło musi się składać z co najmniej 8 znaków długości oraz jednocześnie zawierać małe i wielkie litery, cyfry lub znaki specjalne.
10. W celu zapewnienia odpowiedniego poziomu bezpieczeństwa haseł i innych identyfikatorów pozwalających na autoryzację w programach przetwarzających dane osobowe zaleca się stosowania jakichkolwiek programów i systemów umożliwiających zapamiętywanie identyfikatorów i haseł. Nie ma możliwości zapamiętania hasła użytkownika do systemu operacyjnego.
11. Dostęp do każdego z profili użytkowników ograniczony jest wyłącznie do jednego pracownika.

Parafa:	

12. Zakazuje się kopiowania baz danych z danymi osobowymi na nośniki nieautoryzowane przez Administratora Bezpieczeństwa Informacji i wynoszenia ich poza obszar przetwarzana danych osobowych w wymieniony w Polityce Bezpieczeństwa.

4. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU

4.1. PROCEDURA ROZPOCZĘCIA PRACY PRZEZNACZONA DLA UŻYTKOWNIKA SYSTEMU

Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy, każdy pracownik jest obowiązany do zwrócenia bacznej uwagi, czy nie wystąpiły objawy, mogące świadczyć o naruszeniu zasad ochrony danych osobowych.

Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje uruchomienie komputera, wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu. Użytkownikowi nie wolno w czasie uruchamiania systemu operacyjnego odchodzić od stanowiska. Jest to dozwolone tylko i wyłącznie zgodnie z procedurą opisującą tryb zawieszenia pracy z systemem, w którym przetwarzane są dane osobowe.

Użytkownik informuje Administratora Systemów Informatycznych lub osobę przez niego upoważnioną do opieki nad sprzętem komputerowym o wszelkich nieprawidłowościach w dostępie do systemu informatycznego.

4.2. PROCEDURA ZAWIESZENIA PRACY PRZEZNACZONA DLA UŻYTKOWNIKA SYSTEMU

1. W przypadku konieczności zawieszenia pracy w systemie informatycznym z powodu tymczasowego opuszczenia stanowiska pracy, użytkownik zobowiązany jest, w zależności od przewidywanego okresu swojej nieobecności, do aktywowania wygaszacza ekranu, zabezpieczonego hasłem lub do zablokowania dostępu do użytkowanego systemu komputerowego, np. poprzez jednoczesne naciśnięcie klawiszy {Ctrl + Alt + Delete} i potwierdzenia klawiszem Enter podświetlonej opcji „Zablokuj komputer".

2. Krótkotrwałe przerwy w pracy bez opuszczania stanowiska pracy nie wymagają zamykania aplikacji i wylogowania się z systemu.

4.3. PROCEDURA ZAKOŃCZENIA PRACY PRZEZNACZONA DLA UŻYTKOWNIKA SYSTEMU

Zakończenie pracy polega na wybraniu odpowiedniego polecenia systemowego umożliwiającego zakończenie pracy. Zaleca się zamknięcie wszystkich programów i zapisanie wszystkich otwartych plików. Użytkownik powinien pozostać przy komputerze do chwili jego wyłączenia.

5. PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

1. Kopie zapasowe tworzone są codziennie w sposób automatyczny (dane zapisywane są na serwer oraz zewnętrzne dyski twarde znajdujące się w siedzibie Polskiej Izby Inżynierów Budownictwa). Część danych raz w tygodniu nagrywana jest na zewnętrzne nośniki danych – dyski (HDD).
2. Procedura została opisana w Załączniku nr 1 do Instrukcji.

6. OPIS SPOSOBU, MIEJSCA I OKRESU PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ORAZ KOPII ZAPASOWYCH, O KTÓRYCH MOWA W ROZDZ. 5 INSTRUKCJI

Kopie zapasowe przechowywane są w metalowej szafie zamykanej na klucz w pomieszczeniu [redacted] oraz na serwerze znajdującym się w pomieszczeniu [redacted] w metalowej szafie trwale przytwierdzonej do ściany w siedzibie

Polskiej Izby Inżynierów Budownictwa. Dostęp do obu szaf mają wyłącznie Administrator Systemów Informatycznych oraz upoważnieni przez niego informatycy.
Kopie zapasowe przechowywane są przez 10 lat, chyba że zewnętrzne przepisy wymagają dłuższego okresu przechowywania.

7. OPIS SPOSOBU ZABEZPIECZENIA SYSTEMÓW INFORMATYCZNYCH PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, O KTÓRYM MOWA W PKT III PPKT 1 ZAŁĄCZNIKA DO ROZPORZĄDZENIA

Z uwagi na fakt, iż komputery przetwarzające dane osobowe posiadają dostęp do sieci publicznej, Administrator Danych wdrożył procedury oraz oprogramowanie, które chroni dane osobowe przed nieuprawnionym dostępem, zmianom, usunięciem lub uszkodzeniem. Zagrożenia te to programy zawierające złośliwy kod (wirusy), tzw. konie trojańskie oraz ataki hakerów.

Aby zmniejszyć to zagrożenie, zabronione jest pobieranie oraz instalowanie na komputerach, bez nadzoru Administratora Systemów Informatycznych, jakichkolwiek programów służących do przetwarzania danych osobowych.

Zabronione jest również używanie nośników informacji niepochodzących z zasobów Administratora Danych. Każda osoba przetwarzająca dane osobowe przy użyciu komputera została pouczona, aby w wypadku jakichkolwiek podejrzeń dotyczących obniżenia bezpieczeństwa danych osobowych, poinformowała o tym fakcie osobę upoważnioną przez Administratora Danych lub Administratora Systemów Informatycznych.

Środek sprzętowy infrastruktury informatycznej i telekomunikacyjnej	Uwagi
Zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania	
Dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej/ komputerze przenośnym zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS.	Zabezpieczenie takie stosowane jest na większości stacji

Parafa:	

Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.	
Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł.	
Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.	
Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.	
Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.	
Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej	Stosowane na dwóch komputerach z kopiami baz danych.
Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.	
Użyto system Firewall do ochrony dostępu do sieci komputerowej.	

7.1. ŚRODKI OCHRONY W RAMACH NARZĘDZI PROGRAMOWYCH I BAZ DANYCH

W ramach narzędzi programowych i baz danych zastosowano następujące środki ochrony:

1. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
2. Zainstalowane wygaszacze powinny się uruchamiać po 60 sekundach bezczynności na stanowiskach.
3. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

Parafa:	

8. OPIS SPOSOBU REALIZACJI WYMOGÓW STAWIANYCH SYSTEMOM INFORMATYCZNYM PRZEZ ROZPORZĄDZENIE WYKONAWCZE DO USTAWY O OCHRONIE DANYCH OSOBOWYCH

Nazwa systemu informatycznego / Wymóg rozporządzenia	BUDINFO	SYMFONIA KADRY I PŁACE
System rejestruje datę wprowadzenia danych do systemu	TAK	TAK
System rejestruje identyfikator użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba	TAK	TAK
System rejestruje źródło danych, w przypadku zbierania danych, nie od osoby, której one dotyczą	Brak potrzeby - dane osobowe przetwarzane w ww. systemach pochodzą od osób, których dane te dotyczą.	
System rejestruje informacje o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych	Brak potrzeby - dane osobowe przetwarzane w ww. systemach nie są udostępniane podmiotom trzecim (za wyjątkiem podmiotów opisanych w Polityce Bezpieczeństwa w Rozdziale 8).	
System rejestruje sprzeciw o którym mowa w art. 32 ust. 1 pkt. 8 UODO	TAK	TAK

Parafa:	

9. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

1. O przeprowadzanych przeglądach i konserwacjach systemu informatycznego informowany jest Administrator Bezpieczeństwa Informacji, który może uczestniczyć w dokonywanych czynnościach.
2. Wstępne przeglądy i konserwacje systemów oraz nośników informacji służących do przetwarzania danych a także wstępne czynności serwisowe dokonywane są s siedzibie PIIB.
3. W wypadku wystąpienia takiej potrzeby przegląd i konserwacja mogą być zlecone pracownikowi lub podmiotowi zewnętrznemu specjalizującemu się w tego typu działaniach, Administrator Systemów Informatycznych informuje podmiot, który na podstawie umowy zawartej z Polską Izbą Inżynierów Budownictwa, dokonuje przeglądu i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych, o konieczności podjęcia stosownych czynności
4. W wypadku przekazania sprzętu lub nośników informacji służących do przetwarzania danych osobowych podmiotowi trzeciemu, pozbawia się je zapisanych danych osobowych w sposób, który uniemożliwi ich odtworzenie. W obydwu przypadkach, zostaną zachowane szczególne warunki ostrożności, w celu zabezpieczenia danych osobowych przed dostępem osób nieuprawnionych.
5. Jeśli Administrator Systemów Informatycznych nie dokonuje naprawy osobiście, podmiot dokonujący wyeliminowania opisanych nieprawidłowości, zawiadamia o podjętych czynnościach Administratora Systemów Informatycznych.
6. Wykryte podczas przeglądu i konserwacji nieprawidłowości w działaniu sprzętu lub programów służących do przetwarzania danych osobowych, usuwa się niezwłocznie.
7. Za prawidłowość przeprowadzenia przeglądów i konserwacji systemu informatycznego odpowiada Administrator Systemów Informatycznych.

Parafa:	

10. POZIOM BEZPIECZEŃSTWA

Administrator Danych zastosował środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczył dane osobowe przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

10.1. OKREŚLENIE STOSOWANEGO POZIOMU BEZPIECZEŃSTWA

W zależności od właściwości zbioru danych Administrator Danych stosuje następujące poziomy bezpieczeństwa: podstawowy, podwyższony lub wysoki.

Poziom co najmniej podstawowy stosuje się, gdy w systemie informatycznym nie są przetwarzane dane wrażliwe oraz żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.

Poziom co najmniej podwyższony stosuje się, gdy w systemie informatycznym przetwarzane są dane wrażliwe oraz żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.

Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną.

Jeżeli Administrator Danych stosuje wysoki poziom bezpieczeństwa (pkt 10.2.1 Instrukcji), to oznacza to że realizuje on wymogi określone także przez podstawowy (pkt 10.2.2 Instrukcji) i podwyższony (pkt 10.2.3 Instrukcji) poziom bezpieczeństwa. Analogicznie, jeśli Administrator Danych stosuje podwyższony poziom bezpieczeństwa, to oznacza to że realizuje on wymogi określone także przez podstawowy poziom bezpieczeństwa.

Parafa:	

Nr	NAZWA ZBIORU DANYCH	SYSTEMY INFORMATYCZNE STOSOWANE DO PRZETWARZANIA DANYCH OSOBOWYCH W ZBIORZE	ZASTOSOWANY POZIOM BEZPIECZEŃSTWA
1.	REJESTR CZŁONKÓW PIIB	BUDINFO	Wysoki
2.	REJESTR POTENCJALNYCH CZŁONKÓW PIIB	BUDINFO	Wysoki
3.	REJESTR RZECZOZNAWCÓW	BUDINFO	Wysoki
4.	REJESTR EGZAMINACYJNY	BUDINFO	Wysoki
5.	REJESTR KADROWY KRAJOWEGO BIURA PIIB	SYMFONIA KARDY I PŁACE	Wysoki
6.	REJESTR PROMUJĄCY AKTYWNOŚĆ ZAWODOWĄ CZŁONKÓW PIIB	BARK	Nie dotyczy

10.2. STOSOWANE ZABEZPIECZENIA

10.2.1. POZIOM PODSTAWOWY

Nazwa zabezpieczenia	Stosowanie zabezpieczenia w systemach BUDINFO/ SYMFONIA KADRY I PŁACE
Zabezpieczenie obszaru, w którym przetwarzane są dane osobowe, przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.	TAK / TAK
Przebywanie osób nieuprawnionych, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.	TAK / TAK
Stosowane są mechanizmy kontroli dostępu do danych.	TAK / TAK

Parafa:	

Jeżeli dostęp do danych posiadają co najmniej dwie osoby to w systemie rejestrowany jest dla każdego użytkownika odrębny identyfikator oraz dostęp do danych jest możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.	TAK / TAK
System jest zabezpieczony przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.	TAK / TAK
System jest zabezpieczony przed utratą danych spowodowaną utratą zasilania lub zakłóceniami w sieci zasilającej.	TAK / TAK
Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie jest przydzielany innej osobie.	TAK / TAK
W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 6 znaków.	TAK / TAK
Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych osobowych.	TAK / TAK
Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem oraz usuwa się niezwłocznie po ustaniu ich użyteczności.	TAK / TAK
Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.	TAK / TAK
Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego	TAK / TAK
Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do: 1. likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie. 2. przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie. 3. naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.	TAK / TAK

Parafa:	

10.2.2. POZIOM PODWYŻSZONY

Nazwa zabezpieczenia	Stosowanie zabezpieczenia w systemach BUDINFO/ SYMFONIA KADRY I PŁACE
W przypadku gdy do uwierzytelnienia użytkowników używa się haseł, składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.	TAK / TAK
Urządzenia i nośniki zawierające dane osobowe, zabezpiecza się w sposób zapewniający poufność i integralność tych danych	TAK / TAK

10.2.3. POZIOM WYSOKI

Nazwa zabezpieczenia	Stosowanie zabezpieczenia BUDINFO/ SYMFONIA KADRY I PŁACE
Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.	TAK / TAK
System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.	TAK / TAK

Parafa:	

11. ZAŁĄCZNIKI

Załącznik nr 1 - Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

Dokument sporządzono:	**Pełen podpis Administratora Systemów Informatycznych PIIB:**	**Pieczęć**
Data: …./…./…(dd/mm/rrrr) Miejsce:		

Parafa:	