POLITYKA BEZPIECZEŃSTWA
w Brodnickim Centrum Usług Społecznych

1. Dokumentacja sposobu przetwarzania danych osobowych

1.1 Definicje

Ilekroć w niniejszym dokumencie jest mowa o:

Polityce Bezpieczeństwa, dokumencie – należy przez to rozumieć „Politykę Bezpieczeństwa w Brodnickim Centrum Usług Społecznych;

BCUS – należy przez to rozumieć Brodnickie Centrum Usług Społecznych;

Danych osobowych – oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą");

Osobie możliwej do zidentyfikowania – to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

Zbiorze danych – należy przez to rozumieć każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

Administratorze Danych („**AD**") – należy przez to rozumieć Brodnickie Centrum Usług Społecznych reprezentowane przez Dyrektora;

Inspektorze Ochrony Danych Osobowych („**IOD**") – należy przez to rozumieć osobę wyznaczoną przez AD do nadzorowania przestrzegania zasad ochrony;

Administratorze Systemu Informatycznego („**ASI**") – należy przez to rozumieć osobę wyznaczoną do administrowania systemem informatycznym, informatyk;

Osobie upoważnionej – należy przez to rozumieć: pracownika, współpracownika, wolontariusza, praktykanta, stażystę **-** upoważnionego do przetwarzania danych osobowych przez AD;

Przetwarzaniu danych – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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;

Systemie informatycznym – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

Zabezpieczeniu danych w systemie informatycznym – należy przez to rozumieć wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

Usuwaniu danych – należy przez to rozumieć zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

Zgodzie osoby, której dane dotyczą – oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

Instrukcji – należy przez to rozumieć Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych;

Rozporządzeniu – należy przez to rozumieć Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

1.2 Wprowadzenie

Niniejszy dokument opisuje reguły dotyczące procedur zapewnienia bezpieczeństwa danych osobowych w Brodnickim Centrum Usług Społecznych.
Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę BCUS.

Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym.

Dokument Polityka Bezpieczeństwa wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych i jest w szczególności przeznaczony dla osób pracujących przy przetwarzaniu danych osobowych w BCUS.

Opracowanie „Polityki bezpieczeństwa" wynika z przepisów z Artykułu 24 ust. 1 i jest elementem zapewnienia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z Rozporządzeniem.

1.3 Przepisy ogólne

1. „Polityka bezpieczeństwa” określa tryb postępowania w przypadku, gdy:
1) stan urządzenia, zawartość rejestru danego zbioru danych osobowych, ujawnione metody pracy mogą wskazywać na naruszenie zabezpieczeń tych danych;
2) stwierdzono naruszenie bezpieczeństwa przetwarzanych danych w rejestrze danego zbioru danych.

2. „Polityka bezpieczeństwa” obowiązuje wszystkie osoby pracujące przy przetwarzaniu danych osobowych w BCUS.

3. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa danych BCUS.

4. Administrator Danych, którym Brodnickie Centrum Usług Społecznych reprezentowane przez Dyrektora, powołał Inspektora Ochrony Danych którym jest Pan Rafał Dąbrowski.

5. Administrator Danych upoważnia Inspektora Ochrony Danych do przetwarzania wszystkich zbiorów danych osobowych przetwarzanych.

6. Administrator Danych może w każdym czasie odwołać upoważnienie do przetwarzania danych osobowych udzielone IOD.

7. Odwołanie upoważnienia, o którym mowa w pkt. 6 ma formę pisemną

8. Administrator Danych nadaje upoważnienia do przetwarzania danych osobowych:
pracownikom, wolontariuszom, praktykantom i stażystom.

9. Upoważnienia o których mowa w pkt. 8 mają formę pisemną.

10. AD może w każdym czasie odwołać upoważnienie do przetwarzania danych osobowych udzielone osobom wymienionym w pkt. 8.

11. Odwołanie upoważnień, o których mowa w pkt. 10 ma formę pisemną.

12. Administrator Danych wyznacza Inspektora Ochrony Danych do jego reprezentowania.

13. IOD realizuje zadania w zakresie ochrony danych osobowych, a w szczególności:

1) informuje AD, podmioty przetwarzające oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy Rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradza w tych sprawach;
2) monitoruje przestrzeganie Rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podziału obowiązków, działań zwiększających świadomość, szkoleń personelu uczestniczącego w operacjach przetwarzania oraz powiązanych z tym audytów;
3) udziela na żądanie zalecenia co do oceny skutków ochrony danych oraz monitoruje jej wykonania zgodnie z art. 35 Rozporządzenia;
4) współpracuje z organem nadzorczym;

5) pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 Rozporządzenia, oraz w stosownych przypadkach prowadzi konsultacje we wszystkich innych sprawach.

2. Wykaz pomieszczeń w którym przetwarzane są dane osobowe

Wszystkie pomieszczenia BCUS mają znaczenie dla przetwarzania danych i wsządzie obowiązują zasady ochrony danych.

3. Rejestr czynności przetwarzania danych przez BCUS oraz inne informacje dotyczące przetwarzania danych.

3.1 Rejestr czynności zawiera niezbędne dane umożliwiające realizowanie zadań przez BCUS wynikające z przepisów prawa. Rejestr czynności prowadzi IOD.

3.2 Siedziba BCUS: **ul. Ustronie 2B, 87-300 Brodnica**

3.3 Pomieszczenia, w których przetwarzane są dane osobowe, wyposażone są w szafy drewniane do przechowywania dokumentacji zamykane na klucz.

3.4 Pracownicy mogą przebywać na terenie BCUS w godzinach pracy. Przebywanie w pomieszczeniach poza godzinami pracy dozwolone jest wyłącznie za zgodą Dyrektora. Dostęp do kluczy do budynków posiadają wyłącznie osoby upoważnione przez Dyrektora.

3.5 W BCUS dane mają formę papierową i elektroniczną - są przetwarzane w zasobach systemu informatycznego.

4. Sposób przepływu danych pomiędzy systemami

4.1 BCUS korzysta z oprogramowania dziedzinowego do przetwarzania danych osobowych.

1) Świadczenia Rodzinne (SYGNITY)
2) POMOST (SYGNITY)

BCUS jest administratorem danych a przekazywanie danych odbywa się na zasadzie umowy powierzenia.

4.2 System kadrowo/księgowo/finansowy – RESPONS ZETO OLSZTYN

RESPONS to zintegrowany system informatyczny wspomagający działalność urzędów administracji publicznej i ich jednostek organizacyjnych, wykonany w technologii klient/serwer, polegającej na przeniesieniu operacji obsługi danych na serwer bazy danych, umożliwiającej wzrost wydajności systemu operacyjnego oraz poziomu bezpieczeństwa przetwarzanych danych; zawierający pakiety modułów, stanowiących logicznie wyodrębnione części, ale wzajemnie ze sobą zintegrowanych poprzez wymianę i udostępnianie danych; gwarantujący respektowanie wymagań określonych przepisami prawa,

w szczególności ustaw: o rachunkowości i o ochronie danych osobowych oraz aktów wykonawczych.
RESPONS ułatwia i usprawnia pracę BCUS poprzez; możliwość przekazywania danych pomiędzy poszczególnymi komórkami organizacyjnymi, pracującymi na różnych modułach pakietu w tym samym czasie; znaczne ograniczenie czasu obsługi postępowań; wyeliminowanie konieczności wielokrotnego wprowadzania tych samych danych przez różne komórki organizacyjne urzędu, a także ewentualnej możliwości popełnienia błędów, związanych z ręcznym wprowadzaniem danych; objęcie opieką autorską, która zapewnia stały rozwój oprogramowania i dostosowanie go do potrzeb odbiorcy oraz zmian przepisów prawnych; możliwość pracy zarówno w wersji jednostanowiskowej lub sieciowej.

4.3 Wszystkie podsystemy informatyczne są systemami odrębnymi.

4.3 Programy dziedzinowe wykorzystywane przez BCUS komunikują się z innymi systemami w związku z obowiązującymi przepisami prawa.

5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności przy przetwarzaniu danych osobowych

Administrator danych osobowych jest zobowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych i na nośnikach tradycyjnych, a w szczególności do:

1) zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym,
2) zapobiegania kradzieży danych,
3) zapobiegania przetwarzaniu danych z naruszeniem rozporządzenia oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

5.1 Do zastosowanych środków technicznych należy:

1) przetwarzanie danych osobowych w wydzielonych, odpowiednio zabezpieczonych i przystosowanych do tego pomieszczeniach;

2) stosowanie zabezpieczeń polegających na przechowywaniu dokumentacji bieżącej w szafach zamykanych na zamki w obszarach przetwarzania danych osobowych, oraz przechowywania dokumentacji archiwalnej w specjalnie do tego celu przeznaczonym pomieszczeniu w budynku CWOIRK.

3) ochrona dostępu do danych osobowych przetwarzanych w systemach informatycznych poprzez zastosowanie loginów i haseł uniemożliwiających nieuprawnione korzystanie osobom nieupoważnionym.

5.2 Do zastosowanych przez Administratora Danych i osoby przez niego upoważnione w BCUS środków organizacyjnych służących zapewnieniu poufności, integralności przy przetwarzaniu danych osobowych należy:

1) opracowanie i wdrożenie Polityki Bezpieczeństwa zawierającej również Instrukcję Zarządzania Systemem Informatycznym,

2) wyznaczenie przez AD Inspektora Ochrony Danych (IOD),
3) nadanie pracownikom, praktykantom i stażystom upoważnień do przetwarzania danych osobowych,
4) zaznajomienie osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami dotyczącymi ochrony danych osobowych
5) przeszkolenie osób zatrudnionych przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego
6) zobowiązanie do zachowania tajemnicy przy przetwarzaniu danych osobowych
7) ustawienie monitorów w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane
8) przechowywanie kopii zapasowych zbiorów danych osobowych na innych nośnikach niż podłączone do sieci
9) kontrolowanie dostępu do pomieszczeń BCUS

5.3 Niezależnie od niniejszych zasad, w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie, przy czym dokumenty te nie mogą być sprzeczne z regulacjami określonymi w „Polityce Bezpieczeństwa".

6. AD sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z Rozporządzenia oraz zasad ustanowionych w niniejszym dokumencie.

7. Prawa przysługujące osobie, której dane są przetwarzane:
7.1 Prawo dostępu: Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora następujących informacji:
1) celu przetwarzania;
2) kategorii danych osobowych;
3) informacji o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
4) planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
5) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
6) informacje o prawie wniesienia skargi do organu nadzorczego;
7) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą - wszelkie dostępne informacje o ich źródle;
8) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu
7.2 Prawo do sprostowania danych
7.3 Prawo do usunięcia danych
7.4 Prawo do ograniczenia przetwarzania

8. Dane osobowe udostępnia się na pisemny, umotywowany wniosek. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie. Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

9. Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych

9.1 Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

9.2 Instrukcja dotyczy postępowania w przypadku:

1) naruszenia zabezpieczenia systemu informatycznego lub naruszenia zabezpieczenia danych osobowych zebranych i przetwarzanych w innej formie;

2) podejrzenia że stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.

9.3 Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu bezpieczeństwa danych osobowych, to głównie:
1) **Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu**, jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej, itp.
2) **Niewłaściwe parametry środowiska**, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych.
3) **Awaria sprzętu lub oprogramowania**, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż.
4) **Pojawienie się odpowiedniego komunikatu alarmowego** od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu.
5) **Jakość danych w systemie lub inne odstępstwo** od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie.
6) **Nastąpiło naruszenie lub próba naruszenia** integralności systemu lub bazy danych w tym systemie.
7) **Stwierdzono próbę lub modyfikację danych lub zmianę** w strukturze danych bez odpowiedniego upoważnienia (autoryzacji).
8) **Nastąpiła niedopuszczalna manipulacja danymi osobowymi** w systemie.
9) **Ujawniono osobom nieupoważnionym dane osobowe** lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń.
10) **Praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa** od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.
11) **Ujawniono istnienie nieautoryzowanych kont dostępu** do danych lub tzw. „bocznej furtki", itp.
12) **Podmieniono lub zniszczono nośniki z danymi osobowymi** bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe.
13) **Rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji** (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, prace na danych osobowych w celach prywatnych, itp.).

9.4 Każda osoba w BCUS, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym lub danych przetwarzanych w inny sposób, powinna niezwłocznie poinformować o tym IOD, ASI lub AD.

9.5 Osoba zatrudniona przy przetwarzaniu danych osobowych, która uzyskała informację lub sama stwierdziła naruszenie zabezpieczenia danych osobowych zobowiązana jest niezwłocznie powiadomić o tym IOD, ASI lub AD.

9.6 Dane osobowe zostają ujawnione, gdy stają się znane w całości lub części pozwalającej na określenie osobom nieuprawnionym tożsamości osoby, której dane dotyczą.

9.7 W stosunku do danych, które zostały zagubione, pozostawione bez nadzoru poza obszarem bezpieczeństwa – należy przeprowadzić postępowanie wyjaśniające czy dane osobowe należy uznać za ujawnione.

9.8 Do czasu przybycia na miejsce naruszenia danych osobowych IOD, AD, należy:

1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia (o ile istnieje taka możliwość) a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców naruszenia danych osobowych;
2) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia IOD lub AD.

9.9 Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, IOD lub AD:

1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania, mając na uwadze ewentualne zagrożenia dla prawidłowości pracy organizacji;
2) może żądać dokładnej relacji z zaistniałego naruszenia lub ujawnienia ochrony danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem;
3) rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu lub ujawnieniu ochrony danych osobowych organu nadzorczego;
4) nawiązuje bezpośredni kontakt – jeżeli zachodzi taka potrzeba – ze specjalistami spoza organizacji.

9.10 IOD dokumentuje zaistniały przypadek naruszenia lub ujawnienia ochrony danych osobowych oraz sporządza raport, który powinien zawierać w szczególności:

a) wskazanie osoby powiadamiającej oraz innych osób zaangażowanych lub odpytywanych w związku z naruszeniem lub ujawnieniem ochrony danych osobowych;
b) określenie czasu i miejsca: naruszenia/ujawnienia i powiadomienia o tym fakcie;
c) określenie okoliczności towarzyszących i rodzaju naruszenia/ujawnienia;
d) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania;
e) wstępną ocenę przyczyn wystąpienia naruszenia/ujawnienia;
f) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

Raport IOD niezwłocznie przekazuje AD.

9.11 Analiza, o której mowa w pkt. 9.10, powinna zawierać:
a) wszechstronną ocenę zaistniałego naruszenia/ujawnienia ochrony danych osobowych;
b) wskazanie osób odpowiedzialnych;
c) wnioski co do ewentualnych przedsięwzięć: proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom/ujawnieniom w przyszłości.

10. Instrukcja w sprawie zasad postępowania przy przetwarzaniu danych osobowych - obowiązki osób upoważnionych do przetwarzania danych osobowych

10.1 Instrukcja w sprawie zasad przetwarzania danych osobowych określa w szczególności: **obowiązki osób upoważnionych do przetwarzania danych osobowych** w BCUS.

10.2 AD sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych zapewniając bezpieczeństwo danych osobowych w systemie informatycznym, w szczególności przeciwdziałając dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe oraz podejmując odpowiednie działania w przypadku wykrycia naruszeń w systemie zabezpieczeń.

10.3 IOD i AD współpracują ze sobą przy realizacji zadań z zakresu ochrony danych osobowych.

10.4 Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z Rozporządzeniem. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

10.5 Osoba upoważniona do przetwarzania danych zobowiązana jest do:

1) zapoznania się z obowiązującymi przepisami prawa z zakresu ochrony danych osobowych,
2) zachowania szczególnej staranności przy przetwarzaniu danych osobowych w celu ochrony interesu osób, których dane dotyczą,
3) stosowania określonych przez AD procedur i środków przetwarzania oraz zabezpieczania danych osobowych,
4) podporządkowania się poleceniom IOD i AD w zakresie ochrony danych osobowych,
5) zachowania danych osobowych w tajemnicy,
6) przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa, a w szczególności:
a) zabezpieczenia danych osobowych przed ich utratą, uszkodzeniem lub zniszczeniem,
b) zabezpieczenia danych osobowych przed ich zmianą,
c) zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym,
d) zamykania i zabezpieczania pomieszczeń, w których przetwarzane są dane osobowe w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym,
e) dopilnowania, by przebywanie osób nieupoważnionych w pomieszczeniach, w których przetwarzane są dane osobowe, miało miejsce wyłącznie w obecności osoby upoważnionej,
f) dopilnowania, by przeznaczone do usunięcia dokumenty, zawierające dane osobowe niszczone były w stopniu uniemożliwiającym ich odczytanie,

g) przetwarzania danych osobowych zgodnie z celem, dla którego zostały zebrane,

7) w przypadku stwierdzenia naruszenia zasad postępowania przy przetwarzaniu danych osobowych lub naruszeniu zabezpieczenia danych osoba upoważniona zobowiązana jest niezwłocznie poinformować IOD, który przekazuje tę informację IOD lub bezpośrednio AD.

10.6 Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez AD.

10.7 Upoważnienie udzielane jest na czas wykonywania przez osobę upoważnioną czynności na powierzonym stanowisku.

11. Praca zdalna – obowiązki osób wykonujących pracę zdalną i zasady pracy zdalnej w zakresie ochrony danych

11.1 Za zgodą administratora pracownik może wykorzystywać prywatny komputer lub inne urządzenie do pracy zdalnej w ramach wykonywanych obowiązków służbowych.

11.2 Do przetwarzania danych osobowych są upoważnieni wyłącznie pracownicy.

11.3 Pracownik nie udziela dostępu do komputera, telefonu i innych nośników przekazanych przez Administratora oraz informacji w nich zawartych, w tym danych osobowych, domowników oraz innych osób trzecich.

11.4 Nie wolno udostępniać danych do nawiązania połączenia zdalnego oraz informacji związanych z połączeniem zdalnym, domownikom oraz osobom trzecim.

11.5 Należy zachować poufność danych. Wszelkie notatki i dokumenty należy przechowywać zabezpieczone, tak by osoby trzecie nie miały do nich dostępu.

11.6 Nie można kopiować/zapisywać danych służbowych na niezabezpieczone/ prywatne nośniki pamięci.

11.7 Należy zachować świadomość, że komputer, telefon i inne nośniki przekazane i przez Pracodawcę służą wyłącznie do pracy służbowej – nie wolno instalować dodatkowego oprogramowania bez nadzoru ASI, nie można korzystać ze służbowego sprzętu w innych celach niż te związane z pracą.

11.8 Komputer oraz nośniki udostępnione zabezpiecza się w odpowiedni sposób przed dostępem osób nieupoważnionych, zgodnie z przekazanymi w tym zakresie wytycznymi.

11.9 Należy przestrzegać zasad korzystania z komputera, telefonu i innych nośników wykorzystywanych podczas pracy zdalnej zgodnie z obowiązującymi w tym zakresie procedurami, w tym w szczególności zgodnie z wytycznymi i regulaminami IT.

11.10 Pracownik jest zobowiązany zwrócić powierzone nośniki wraz z danymi na każde żądanie Administratora.

11.11 Podczas pracy zdalnej obowiązują zasady Polityki Bezpieczeństwa oraz Instrukcji

12. INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

12.1 Dodatkowe definicje

Integralność danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

Uwierzytelnianie – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

Identyfikator użytkownika – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

Hasło – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

System informatyczny – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

12.3 Uprawnienia do przetwarzania danych – nadawanie oraz rejestracja w systemie

12.3.1 Do obsługi systemu informatycznego służącego do przetwarzania danych osobowych może być dopuszczona wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych.

12.3.2 ASI rejestruje uprawnienia w systemach informatycznych. ASI jest odpowiedzialny za administrację użytkownikami w systemie informatycznym.

12.3.3 Upoważnienia do przetwarzania danych osobowych przechowywane są w teczkach akt osobowych pracowników.

12.3.4 Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora użytkownika i właściwego hasła.

12.3.5 Dla każdego użytkownika systemu informatycznego, który przetwarza dane osobowe, ASI ustala niepowtarzalny identyfikator i hasło początkowe.

12.3.6 Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego, nie powinien być przydzielany innej osobie.

12.3.7 W przypadku utraty przez osobę uprawnienia dostępu do danych osobowych należy niezwłocznie zablokować dostęp do systemu informatycznego.

12.3.8 ASI przekazuje użytkownikowi identyfikator i hasło dostępu do systemu.

12.3.9 IOD przeprowadza szkolenie z zakresu pracy w systemie informatycznym oraz bezpieczeństwa danych w systemie informatycznym.

12.3.10 Użytkownik ma obowiązek zapoznania się z instrukcją oprogramowania dziedzinowego wykorzystywanego do realizacji swoich obowiązków oraz śledzenia zmian w tej instrukcji.

12.4 Uwierzytelnianie – metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

12.4.1 Dane osobowe przetwarzane są w BCUS z użyciem komputerów.

12.4.2 Hasło użytkownika powinno mieć minimum 8 znaków i być zmieniane nie rzadziej niż raz w miesiącu.

12.4.3 Hasło powinno zawierać małe i duże litery oraz przynajmniej jeden znak specjalny.

12.4.4 Hasło nie może zawierać żadnych informacji, które można łatwo skojarzyć z użytkownikiem komputera. Zakazuje się zapisywania hasła w miejscu dostępnym dla osób nieupoważnionych. Użytkownik nie może udostępniać nikomu swojego hasła.

12.4.5 Hasło nie może być zapisywane w przeglądarkach internetowych lub innych narzędziach.

12.4.6 Hasło użytkownika stosowane do uwierzytelniania w systemie informatycznym należy utrzymywać w tajemnicy nawet po upływie jego ważności.

12.4.7 Identyfikator przydzielony osobie nie może być wykorzystany w celu nadania go drugiej osobie.

12.4.8 Nowy użytkownik otrzymuje identyfikator oraz hasło początkowe, które zobowiązany jest zmienić na znane tylko sobie.

12.4.9 W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest do natychmiastowej zmiany hasła.

12.5 Procedury rozpoczęcia, zawieszenia oraz zakończenia pracy

12.5.1 Rozpoczęcie pracy użytkownika w systemie informatycznym następuje po poprawnym uwierzytelnieniu (zalogowaniu się do systemu).

12.5.2 Praca w aplikacjach prowadzona jest zgodnie z instrukcją zawartą w dokumentacji aplikacji.

12.5.3 Zakończenie pracy użytkownika następuje po poprawnym wylogowaniu się z systemu oraz poprzez uruchomienie odpowiedniej dla danego systemu opcji jego zamknięcia.

12.5.4 Użytkownik ma obowiązek wylogowania się bądź zablokowania dostępu do systemu w przypadku zaplanowanej dłuższej nieobecności na stanowisku pracy. Niedopuszczalne jest pozostawienie stanowiska komputerowego z uruchomionym i dostępnym systemem bez nadzoru.

12.5.5 Monitory stanowisk komputerowych znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych należy ustawić w taki sposób, aby uniemożliwić osobom postronnym wgląd w dane.

12.5.6 Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na obszarze, w którym przetwarzane są dane osobowe jest dozwolone tylko w obecności osób uprawnionych do ich przetwarzania, bądź za wiedzą i zgodą IOD.

12.5.7 Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać na czas nieobecności osób uprawnionych, uniemożliwiając dostęp osobom trzecim.

12.5.8 W przypadku braku możliwości zalogowania się do systemu należy niezwłocznie poinformować ASI o tym zdarzeniu.

12.5.9 W przypadku stwierdzenia lub podejrzenia fizycznej ingerencji w przetwarzane dane osobowe lub używane narzędzia programowe lub sprzętowe należy niezwłocznie zaprzestać używania sprzętu a następnie powiadomić ASI.

12.5.10 Wszelkie problemy z zakończeniem działania programów lub systemu operacyjnego należy zgłaszać Administratorowi Systemu Informatycznego.

12.6 Sposoby zabezpieczenia urządzeń systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieautoryzowanego dostępu do systemu informatycznego

12.6.1 Komputery i systemy pracujące w BCUS muszą posiadać zainstalowany program antywirusowy oraz oprogramowanie i mechanizmy zabezpieczające przed nieautoryzowanym dostępem z sieci publicznej.

12.6.2 Każdy komputer z dostępem do Internetu musi być zabezpieczony za pomocą programu antywirusowego.

12.6.3 Zainstalowany program antywirusowy powinien być tak skonfigurowany, by aktualizował bazy wirusów oraz zapewniał ochronę plików w czasie rzeczywistym.

12.6.4 W przypadku, gdy użytkownik stanowiska komputerowego zauważy komunikat oprogramowania zabezpieczającego system wskazujący na zaistnienie zagrożenia zobowiązany jest zaprzestać jakichkolwiek czynności w systemie i niezwłocznie skontaktować się z ASI.

12.6.5 Zabrania się użytkownikom blokowania, wyłączania oraz odinstalowywania programów zabezpieczających komputer przed złośliwym oprogramowaniem oraz nieautoryzowanym dostępem z sieci.

12.7 Procedury tworzenia kopii zapasowych zbiorów danych osobowych oraz programów i narzędzi służących do ich przetwarzania

12.7.1 Zbiory danych w systemie informatycznym są zabezpieczone przed utratą lub uszkodzeniem za pomocą urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej oraz poprzez sporządzanie kopii zapasowych zbiorów danych.

12.7.2 Za tworzenie kopii bezpieczeństwa Systemu Informatycznego odpowiedzialny jest ASI.

12.7.3 Częstotliwość tworzenia pełnych kopii zapasowych zbiorów danych ustala ASI.

12.7.4 Kopie baz danych tworzy się na dysku w pomieszczeniu innym niż to w którym znajdują się wykorzystywane bazy danych programów oraz na dysku do tego przeznaczonym podłączanym do sieci tylko w celu wykonania kopi zapasowej.

12.7.5 Kopie przechowywane w warunkach uniemożliwiających dostęp do nich osobom niepowołanym.

12.7.6 Kopie są okresowo sprawdzane pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu oraz usuwane po ustaniu ich użyteczności. Decyzje o usunięciu kopii-awaryjnej podejmuje ASI.

12.8 Wykonywanie przeglądów oraz konserwacji urządzeń oraz nośników informacji służących do przetwarzania danych osobowych

12.8.1 Przeglądu i konserwacji systemów informatycznych i zbiorów danych osobowych dokonuje ASI lub osoby przez niego wyznaczone sprawdzając poprawność pracy systemu ze zbiorem danych informując o tym fakcie IOD.

12.8.2 Naprawa sprzętu na którym znajdują się dane osobowe odbywa się za wiedzą IOD. W przypadku gdy zadanie to Administrator powierzy podmiotowi zewnętrznemu, informuje o tym fakcie IOD oraz konsultuje z nim zakres powierzenia danych osobowych.

12.8.3 Bezpieczeństwo danych osobowych w odniesieniu do napraw sprzętu czy systemów informatycznych.

Nośniki zawierające dane osobowe można przekazać do naprawy pod warunkiem, podpisania umowy powierzenia danych z podmiotem który miałby dokonywać naprawy/przeglądu. Podmiot z którym podpisuje się umowę powierzenia musi zagwarantować spełnienie zasad bezpieczeństwa przetwarzania danych osobowych oraz przestrzegać obowiązujących przepisów prawa w tym w szczególności Rozporządzenia. Umowa powierzenia konsultowana jest z IOD.

Warunki wymienione powyżej obowiązują również przy dokonywaniu napraw systemów informatycznych przez podmioty zewnętrzne oraz przy konsultacjach z podmiotami zewnętrznymi dotyczącymi systemów informatycznych w przypadku przekazywania danych osobowych.

12.9 Sposób, miejsce oraz okres przechowywania kopii zapasowych i elektronicznych nośników informacji zawierających dane osobowe

12.9.1 Kopie zapasowe tworzone są w wyznaczonym do tego pomieszczeniu - serwerowni.

12.9.2 Kopie wykonuje się na nośnikach podłączonych do sieci oraz na nośnikach zewnętrznych przyłączanych do sieci podczas tworzenia kopii.

12.9.3 Okres przechowywania kopii zapasowych określa ASI z uwzględnieniem obowiązujących przepisów.

12.10 Użytkownikom systemu informatycznego w którym przetwarzane są dane osobowe zabrania się

1) Ujawniania hasła i identyfikatora (loginu) współpracownikom oraz osobom trzecim.

2) Przechowywania haseł w miejscu widocznym bądź łatwo dostępnym dla innych osób w tym też zapisywania haseł w przeglądarkach internetowych lub innych narzędziach informatycznych.

3) Udostępniania stanowisk pracy wraz z danymi osobowymi osobom nieuprawnionym.

4) Udostępniania osobom nieuprawnionym programów komputerowych.

5) Używania programów w innym zakresie niż pozwala na to umowa licencyjna oraz zakres obowiązków.

6) Przenoszenia oprogramowania bez wiedzy i zgody ASI.

7) Tworzenia kopii danych na zewnętrznych nośnikach w celu wyniesienia ich poza obszar BCUS.

8) Instalowania i używania jakichkolwiek programów komputerowych (w tym również programów do użytku prywatnego) bez wiedzy i zgody AD.

9) Używania nośników danych niewiadomego pochodzenia oraz nośników innych niż dopuszczone przez AD

10) Pozostawiania otwartych dokumentów na ekranie monitora bez blokady dostępu.

11) Pozostawiania dokumentów bądź kopii dokumentów zawierających dane osobowe w drukarkach bądź kserokopiarkach.

12) Wyrzucania dokumentów zawierających dane osobowe bez uprzedniego trwałego zniszczenia.

13) Przekazywania danych osobowych osobom nieupoważnionym. Dane osobowe mogą być udostępnianie zgodnie z obowiązującymi przepisami na pisemny wniosek.

14) Ignorowania zapisów Polityki Bezpieczeństwa.

15) Logowania do systemu na urządzeniach nie zapewniających odpowiedniego poziomu bezpieczeństwa ochrony danych osobowych – w tym również logowania na komputerach nie zabezpieczonych programem antywirusowych lub z nieaktualnym oprogramowaniem antywirusowym.

16) Logowania się podczas pracy i pracy na urządzeniach mobilnych podłączonych do niezabezpieczonych sieci, sieci publicznych.

17) Utrwalania danych na urządzeniach, w tym również na urządzeniach mobilnych, chyba że jest to związane bezpośrednio z wykonywaniem obowiązków służbowych (przechowywanie informacji).

18) Przesyłania danych osobowych w niezaszyfrowanej postaci (dotyczy między innymi wysyłania danych w postaci maili lub ich załączników, przesyłania niezabezpieczonych hasłem plików)

19) Wynoszenia sprzętu poza siedzibę organizacji bez uzyskania wcześniejszego zezwolenia od AD

12.11 Komunikacja z innymi systemami informatycznymi.

11.1 Programy dziedzinowe wykorzystywane przez BCUS komunikują się z innymi systemami w związku z obowiązującymi przepisami prawa.
11.2 Oprogramowania dziedzinowe zapewnia niezbędne zabezpieczenia komunikacji pomiędzy systemami.
11.3 W razie podejrzenia nieprawidłowości w komunikacji, niepoprawnego działania lub innych problemów pracownik powiadamia ASI.

12.12 Wszelkie przypadki naruszenia niniejszej Instrukcji należy zgłaszać IOD lub bezpośredniemu przełożonemu który zawiadamia IOD i AD.