**ZARZĄDZENIE**
**Dyrektora**
**Zakładu Usług Komunalnych w Węglińcu, ul. Partyzantów, 59-940 Węgliniec**

**Nr 02/2022**
**z dnia 12.10.2022r.**

w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Zakładzie Usług Komunalnych w Węglińcu, ul. Partyzantów, 59-940 Węgliniec reprezentowany przez Dyrektora.

§ 1.

Działając w oparciu o rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L119 z 4 maja 2016 r.)

zarządzam

§ 2.

wprowadzenie Polityki Bezpieczeństwa Informacji oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Zakładzie Usług Komunalnych w Węglińcu, ul. Partyzantów, 59-940 Węgliniec,

stanowiące odpowiednio załącznik nr 1 oraz załącznik nr 2 do niniejszego Zarządzenia.

§ 3.

Wzór oświadczenia pracowników o zapoznaniu się z ww. dokumentami stanowi załącznik nr *3* do niniejszego Zarządzenia.

§ 4.

Jednocześnie traci ważność zarządzenie nr 2/2018 z dnia 29.03.2018r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji i Instrukcji zarządzania systemem informatycznym w Zakładzie Usług Komunalnych w Węglińcu, ul. Partyzantów, 59-940 Węgliniec

§ 5.

Zarządzenie wchodzi w życie po upływie 14 dni od wydania, z dniem 26.10.2022r.

DYREKTOR
Zakładu Usług Komunalnych w Węglińcu
mgr inż. Krzysztof Polewski

Data i podpis Dyrektora

Załącznik Nr 1
do Zarządzenia
Dyrektora
Nr 02/2022
z dnia 12.10.2022

# POLITYKA BEZPIECZEŃSTWA INFORMACJI

## w Zakładzie Usług Komunalnych w Węglińcu

## ul. Partyzantów 8 Węgliniec, 59-940 Węgliniec

*Zatwierdzam do stosowania*

DYREKTOR
Zakładu Usług Komunalnych w Węglińcu
mgr inż. Krzysztof Polewski

## SPIS TREŚCI

## Rozdział 1.
## Postanowienia ogólne

### § 1.

### Słownik pojęć

1. **Administrator Danych Osobowych** (**ADO**) - Zakład Usług Komunalnych w Węglińcu, ul. Partyzantów 8, 59-940 Węgliniec reprezentowany przez Dyrektora.
2. **Inspektor Ochrony Danych Osobowych (IOD)** - osoba fizyczna upoważniona przez Administratora Danych Osobowych, zajmująca się zapewnianiem przestrzegania przepisów o ochronie danych osobowych oraz prowadzeniem wymaganej prawem dokumentacji związanej z przetwarzaniem tych danych przez administratora;
3. **Baza danych osobowych** – zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci wewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze – rekordów lub obiektów, w których są zapisywane dane osobowe;
4. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne;
5. **ZUK** – Zakład Usług Komunalnych w Węglińcu, ul. Partyzantów 8, 59-940 Węgliniec reprezentowany przez Dyrektora
6. **Administrator Systemów Informatycznych (ASI)** – osoba fizyczna wyznaczona przez Administratora Danych Osobowych, zajmująca się sprawowaniem ogólnego nadzoru nad bezpieczeństwem organizacyjnym, fizycznym oraz technicznym danych osobowych przetwarzanych w systemie informatycznym;
7. **UODO** – Urząd Ochrony Danych Osobowych – organ nadzorczy w stosunku do administratorów danych osobowych;
8. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, uwierzytelniający osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
9. **Identyfikator Użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
10. **Incydent** - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji lub zmniejszeniem poziomu usług systemowych, które stwarzają znaczne prawdopodobieństwo zakłócenia działania systemu informatycznego i zagrażają bezpieczeństwu informacji; naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność;
11. **Nośniki danych** – przedmioty fizyczne (elektroniczne, papierowe), na których możliwe jest zapisanie informacji w celu ich przechowywania, przetwarzania i transmisji. Każdy nośnik danych charakteryzuje określona gęstość zapisu, wynikająca z jego właściwości fizycznych;

12. **Odbiorca danych** – każdy, komu udostępniane są dane osobowe, z wyłączeniem: osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, przedstawiciela administratora danych mającego siedzibę w państwie trzecim, przetwarzającego dane przy wykorzystaniu środków technicznych znajdujących się na terytorium RP podmiotu, który przetwarza dane na podstawie umowy powierzenia zawartej z administratorem, a także organów państwowych i organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;
13. **Podatność** - luka (słabość), która może być wykorzystana, przez co najmniej jedno zagrożenie, rozumiane jako potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę;
14. **PBI / Polityka** – niniejszy dokument;
15. **Przepisy prawa** – obowiązujące przepisy prawa w zakresie ochrony danych osobowych;
16. **Pracownik** – osoba fizyczna świadcząca na rzecz administratora pracę na podstawie stosunku pracy, powołania, mianowania, wykonująca zadania wyłącznie osobiście, w ramach prowadzonej działalności gospodarczej lub powierzone jej na podstawie umowy cywilnoprawnej, współpracująca w rozumieniu obowiązującej ustawy o systemie ubezpieczeń społecznych.
17. **Przetwarzane danych** – wszelkie operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te operacje, które wykonuje się w systemie informatycznym;
18. **System informatyczny (system IT)** - zespół współpracujących ze sobą urządzeń, programów, systemów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
19. **System tradycyjny** - zespół procedur organizacyjnych, wyposażenia i środków trwałych związanych z mechanicznym przetwarzaniem informacji zawierających dane osobowe na nośnikach papierowych;
20. **Sieć publiczna** – sieć telekomunikacyjna wykorzystywana głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych;
21. **Teletransmisja** – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
22. **Usługi świadczone drogą elektroniczną** – wszystkie usługi, których wykonanie następuje przez wysyłanie i odbieranie danych za pomocą systemów teleinformatycznych na indywidualne żądanie usługobiorcy (klienta), bez jednoczesnej obecności stron, transmitowanych za pośrednictwem sieci publicznych.
23. **Użytkownik** – każda osoba, która uzyskała upoważnienie od ADO do przetwarzania danych osobowych w systemie informatycznym, a także osoba upoważniona przez podmiot, z którym została podpisana umowa powierzenia przetwarzania danych osobowych;
24. **Zabezpieczenie danych w systemie informatycznym** - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
25. **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

## § 2.
## Cel i zakres stosowania Polityki Bezpieczeństwa Informacji.

1. Polityka Bezpieczeństwa Informacji jest wewnętrznym dokumentem regulującym zasady przetwarzania i ochrony danych osobowych w ZUK;
2. Polityka Bezpieczeństwa Informacji została opracowana i wdrożona w celu uzyskania standardu przetwarzania informacji zawierających dane osobowe zgodnego z wymaganiami określonymi w obowiązujących przepisach prawa, danych osobowych przetwarzanych w systemie informatycznym oraz pozostałych informacji podlegających ochronie;
3. Niniejsza Polityka została udostępniona każdej osobie mającej dostęp do danych osobowych przetwarzanych w ZUK w formie tradycyjnej (papierowej) oraz w systemie informatycznym;
4. Potwierdzeniem zapoznania się z postanowieniami niniejszego dokumentu jest złożenie pisemnego oświadczenia (załącznik nr 3 do Zarządzenia). Złożone oświadczenie winno być wpięte do akt osobowych pracownika lub dołączone do zawartej umowy cywilnoprawnej.

## § 3.

Niniejsza Polityka Bezpieczeństwa Informacji określa w szczególności:

a) prawa, obowiązki oraz granice dopuszczalnego zachowania osób przetwarzających dane osobowe, Użytkowników systemu IT i tradycyjnego, w których przetwarzane są dane osobowe oraz konsekwencje naruszenia przepisów o ochronie danych osobowych;
b) sposób przetwarzania danych osobowych oraz środki organizacyjne i techniczne zapewniające ochronę tych danych, w tym podstawowe warunki jakim powinny odpowiadać urządzenia z wykorzystaniem których dane są przetwarzane;
c) zasady prowadzenia dokumentacji związanej z przetwarzaniem danych osobowych;
d) wymagania w zakresie odnotowywania udostępniania danych osobowych;
e) instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych;
f) instrukcję bezpiecznego przetwarzania danych osobowych w systemie IT.

## § 4.

Zastosowane zabezpieczenia mają zapewnić:

1. **poufność danych** – rozumianą jako właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym osobom;
2. **integralność danych** – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
3. **rozliczalność danych** - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
4. **integralność systemu** - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji zamierzonej, jak i przypadkowej;
5. **dostępność informacji** - rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
6. **zarządzanie ryzykiem** - rozumiane jako proces identyfikowania, monitorowania, minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa informacji, które może dotyczyć systemów informatycznych i tradycyjnych służących do przetwarzania danych osobowych.

## Rozdział 2.
## Administrator Danych Osobowych. Inspektor Ochrony Danych Osobowych (IOD). Administrator Systemów Informatycznych (ASI).

### § 5.
### Administrator Danych Osobowych (ADO)

1. Administrator Danych Osobowych podejmuje decyzje w zakresie realizacji celów i zapewnienia środków zapewniających bezpieczeństwo przy przetwarzaniu danych osobowych, zgodnie z wymogami i zaleceniami wynikającymi z przepisów prawa, w celu ochrony interesów osób, których dane dotyczą;
2. Administrator Danych Osobowych pełni funkcję kontrolną w zakresie poprawnego przetwarzania danych osobowych oraz nadzoruje przestrzeganie ustalonych zasad zawartych w niniejszej Polityce;
3. Administrator Danych Osobowych powołuje Inspektora Ochrony Danych (IOD) zgodnie z przepisami obowiązującymi w zakresie ochrony danych;
4. W przypadku niepowołania IOD, funkcje mu przypisane ADO pełni w zakresie zgodnym z obowiązującymi przepisami;

### § 6.

Zadania nałożone na Administratora Danych Osobowych przepisami obowiązującymi w zakresie ochrony danych osobowych obejmują ponadto:

a) rzetelne i przejrzyste wypełnienie obowiązku informacyjnego;
b) wykazanie, że zastosowane środki techniczne i organizacyjne zapewniają należyty poziom ochrony danych osobowych oraz, że dane osobowe przetwarzane są zgodnie z zasadami zgodności z prawem, ograniczenia, minimalizacji danych, prawidłowości, ograniczenia przechowywania, integralności i poufności i prawidłowości przetwarzania danych osobowych;
c) dokonywanie oceny ryzyka naruszenia praw i wolności osób, których dane osobowe są przetwarzane z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania danych osobowych. Ocena ryzyka jest konieczna dla wdrożenia przez ZUK właściwych środków technicznych i organizacyjnych, zapewniających bezpieczeństwo przetwarzanych danych osobowych;
d) nadawanie i anulowanie upoważnień do przetwarzania danych osobowych,
e) dbałość o ochronę danych osobowych już na etapie projektowania wdrażanych rozwiązań związanych z przetwarzaniem danych;
f) prowadzenie rejestru czynności przetwarzania danych osobowych, zgodnie z wzorem stanowiącym załącznik do PBI;
g) zgłaszanie do organu nadzorczego faktu naruszenia ochrony danych osobowych, nie później niż po upływie 72 godzin.

### § 7.
### Inspektor Ochrony Danych Osobowych (IOD)

Inspektor Ochrony Danych (IOD) jest powoływany przez Administratora danych Osobowych drogą pisemnego upoważnienia. Wzór upoważnienia dla IOD stanowi załącznik do PBI.
IOD jest również zobowiązany do podpisania oświadczenia o zachowaniu poufności.

§ 8.

1. Do kompetencji IOD należy w szczególności:
   a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowywanie w tym zakresie sprawozdań dla ADO,
   b) nadzorowanie przestrzegania zasad ochrony danych osobowych tj. środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, ze szczególnym uwzględnieniem zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, w tym nadzór nad obiegiem oraz przechowywaniem materiałów i dokumentów zawierających dane osobowe
   c) współpraca z ASI w zakresie dotyczącym przetwarzania danych osobowych w systemie informatycznym,
   d) nadzorowanie opracowania i aktualizacji dokumentacji opisującej sposób przetwarzania danych, środki ich ochrony oraz przestrzegania zasad w niej określonych,
   e) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
   f) wnioskowanie i opiniowanie wniosków do ADO o nadanie, zmianę lub cofnięcie uprawnień dostępu do danych osobowych oraz pozostałych wniosków dotyczących bezpieczeństwa informacji, w tym danych osobowych, a także nadzór w zakresie realizacji tych wniosków,
   g) we współpracy z ADO, nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe oraz organizacją kontroli przebywających w nich osób,
   h) zapewnienie przeciwdziałania incydentom oraz prowadzenie rejestru zdarzeń (załącznik do PBI),
   i) zapewnienie edukacji pracowników (w tym Użytkowników systemu IT) na temat zasad ochrony danych osobowych i polityki bezpieczeństwa informacji stosowanej w ZUK poprzez wnioskowanie do ADO o systematyczne szkolenia w tym zakresie oraz bieżące monitorowanie poziomu wiedzy pracowników, np. poprzez cykliczne przeprowadzanie testów sprawdzających (przynajmniej raz w roku);
   j) informowanie administratora oraz pracowników o obowiązkach spoczywających na nich na mocy przepisów prawa,
   k) monitorowanie przestrzegania przepisów krajowych oraz Unii i państw członkowskich oraz polityk administratora lub procesora,
   l) szkolenie personelu uczestniczącego w operacjach przetwarzania danych osobowych,
   m) przeprowadzanie systematycznych audytów wewnętrznych,
   n) udzielanie wskazówek Administratorowi Danych Osobowych w przedmiocie wdrożenia odpowiednich i skutecznych środków technicznych jak również organizacyjnych mających zabezpieczyć dane osobowe,

o) udzielanie wskazówek Administratorowi Danych Osobowych, jak wykazać przestrzeganie prawa w zakresie identyfikowania ryzyka związanego z przetwarzaniem danych osobowych, jego oceny pod kątem źródła, charakteru, prawdopodobieństwa i wagi zagrożenia oraz w zakresie najlepszych praktyk pozwalających zminimalizować to ryzyko,
p) udzielanie zaleceń w zakresie oceny skutków oraz monitorowanie ich wykonania w przypadku, gdy administrator danych przed rozpoczęciem przetwarzania zobowiązany jest do przeprowadzenia oceny skutków planowanych operacji przetwarzania dla ochrony danych,
q) utrzymywanie stałej współpracy z organem nadzorczym,
r) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
s) prowadzenie rejestru czynności przy przetwarzaniu danych osobowych, za które odpowiada administrator danych i rejestru kategorii czynności przetwarzania danych dokonywanych w imieniu administratora przez podmiot przetwarzający.

**§ 9.**

1. Inspektor Ochrony Danych Osobowych prowadzi rejestr czynności przy przetwarzaniu danych osobowych.
2. W ramach nadzoru nad przetwarzaniem danych osobowych, IOD sprawdza cele, zakres przetwarzania, czas przetwarzania oraz sposoby zabezpieczenia tych danych, w tym w porozumieniu z ASI, zabezpieczenia urządzeń mobilnych wykorzystywanych w ZUK;
2. IOD jest również zobowiązany do przeprowadzania analizy ryzyk związanych z zagrożeniami związanymi z przetwarzaniem danych osobowych w systemie informatycznym oraz tradycyjnym, z uwzględnieniem specyfiki pracy wiążącej się z koniecznością przetwarzania danych osobowych poza siedzibą ZUK z wykorzystaniem urządzeń mobilnych. Dokumentację analizy IOD przedstawia ADO w celu dokonania oceny ryzyka i podjęcia stosownych działań;

**§ 10.**

ZUK, jako Administrator Danych Osobowych, gwarantuje IOD niezależność oraz podległość najwyższemu kierownictwu tak, aby IOD mógł bezpośrednio kontaktować się z osobami decyzyjnymi w sprawie przetwarzania danych osobowych oraz mieć dostęp do wszystkich informacji, które związane są z przetwarzaniem danych osobowych.

**§ 11.**

IOD jest właściwie i niezwłocznie angażowany we wszystkie sprawy dotyczące ochrony danych osobowych przetwarzanych w ZUK, tzn. uczestniczy we wszystkich pracach, które mogą wpływać na kształt operacji związanych z przetwarzaniem danych osobowych (art. 35 ust. 2 RODO).

## § 12.
## Administrator Systemów Informatycznych.

1. Do zadań ASI należy zapewnienie działania infrastruktury teleinformatycznej i oprogramowania w sposób zapewniający właściwy poziom bezpieczeństwa informacji wynikający z obowiązujących przepisów, PBI oraz zaleceń IOD;
2. Nadzorowanie przez ASI przestrzegania bezpieczeństwa danych osobowych gromadzonych i przetwarzanych w systemie IT ma na celu zabezpieczenie ich przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
3. Do kompetencji ASI należy w szczególności:
   a) zapewnienie właściwego poziomu bezpieczeństwa systemu informatycznego, w tym danych osobowych w nim przetwarzanych,
   b) zapewnienie mechanizmów uwierzytelniania użytkowników w systemie informatycznym służącym do przetwarzania danych osobowych oraz kontrola dostępu do tych danych,
   c) inicjatywa w zakresie zapewnienia alternatywnego, awaryjnego zasilania systemu informatycznego oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych, w tym raportowanie do IOD stanu zabezpieczeń w zakresie centralnego awaryjnego zasiania budynku, w porozumieniu z administratorem budynku,
   d) podejmowanie działań zabezpieczających system informatyczny w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu, informacji o zmianach w sposobie działania systemu lub innych urządzeń wskazującej na naruszenie bezpieczeństwa danych,
   e) zapewnienie ochrony systemu teleinformatycznego oraz danych osobowych przesyłanych za pośrednictwem tego systemu,
   f) zapewnienie ochrony danych osobowych w związku z naprawą, konserwacją oraz likwidacją systemu informatycznego, w tym urządzeń komputerowych i mobilnych, na których zapisane są dane osobowe,
   g) wnioskowanie i opiniowanie wniosków do ADO o nadanie, zmianę lub cofnięcie uprawnień dostępu do danych osobowych w systemie informatycznym oraz realizacja tych czynności po akceptacji ADO,
   h) zapewnienie przeglądów, konserwacji oraz uaktualnień systemu służącego do przetwarzania danych osobowych z uwzględnieniem specyfiki funkcjonowania ZUK;
   i) przestrzeganie przepisów bhp i ppoż. w przynależnych pomieszczeniach.

## Rozdział 3.
## Zasady przetwarzania danych osobowych. Profilowanie. Powierzenie. Udostępnianie. Obowiązek informacyjny. Zgoda. Zabezpieczenia. Sprawdzenia. Odpowiedzialność.

### § 13.
### Zasady przetwarzania danych osobowych.

1. ZUK gromadzi dane osobowe swoich pracowników, kandydatów do pracy, dzieci, zleceniobiorców, kontrahentów i podmiotów współpracujących (dostawców, usługodawców itp.);
2. ZUK pozyskuje dane osobowe osób, o których mowa w ust. 1 na dwa sposoby:
   a) bezpośrednio od osoby, której dane dotyczą,
   b) z wykorzystaniem innych źródeł niż osoba, której dane dotyczą, w granicach dopuszczalnych przepisami prawa;
3. ZUK przetwarza dane osobowe w sposób adekwatny, stosowny oraz ograniczony do tego, co jest niezbędne w celu realizacji usługi;
4. Wszystkie osoby upoważnione do przetwarzania danych osobowych w ZUK są zobowiązane do zachowania w tajemnicy tych danych poprzez złożenie oświadczenia o zachowaniu poufności nawet po ustaniu zatrudnienia, zakończenia współpracy, wygaśnięciu umowy itd.

### § 14.

1. Uprawnienia do przetwarzania danych osobowych w systemie IT nadawane są zgodnie z właściwą procedurą określoną w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w ZUK. Uprawnienia, o których mowa w zdaniu pierwszym, ważne są do dnia odwołania lub do chwili ustania zatrudnienia uprawnionego pracownika;

2. Ochrona dotyczy w szczególności:

   a) danych osobowych gromadzonych i przetwarzanych w związku z działalnością ZUK, w tym danych osobowych podmiotów współpracujących w związku z zawieranymi umowami,
   b) danych osobowych pracowników, w tym danych osobowych i treści zawieranych umów o pracę,
   c) danych osobowych kandydatów do pracy zbieranych na etapie rekrutacji,
   d) danych osobowych zawartych w dokumentach finansowo-księgowych,
   e) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach IT, w których są przetwarzane dane osobowe,
   f) rejestru osób dopuszczonych do przetwarzania danych osobowych,
   g) danych osobowych zawartych w pozostałych dokumentach wytwarzanych w związku z działalnością ZUK.

3. Katalog przetwarzanych danych osobowych może ulec rozszerzeniu, w zależności od bieżącej działalności ZUK, niemniej musi mieścić się w granicach zgodnych przepisami prawa.

§ 15.

1. Pomieszczenia znajdujące się w siedzibie ZUK podzielone są na:
   a) strefę ogólnodostępną obejmującą pomieszczenia, do których dostęp posiadają pracownicy, goście, dzieci, serwis zewnętrzny oraz pozostałe osoby przebywające w tej strefie w związku z wykonywanymi obowiązkami lub czynnościami,
   b) strefę obejmującą pomieszczenia, gdzie kontrolowany jest ruch osobowy, objęte szczególną kontrolą wejścia i wyjścia oraz przebywania, (kontrolą dostępu), gdzie przebywać mogą wyłącznie upoważnieni pracownicy lub pozostałe osoby pod nadzorem upoważnionych pracowników.

§ 16.

Wszystkie osoby, które posiadają dostęp do danych osobowych w obszarze wymienionym w § 15 ust. 1 pkt 2 muszą posiadać pisemne upoważnienie do przetwarzania danych nadane przez ADO oraz podpisać oświadczenie o zachowaniu poufności. Wzory upoważnienia i oświadczenia stanowią załączniki do PBI.

§ 17.

1. W zbiorach danych gromadzonych w systemie informatycznym **zabrania się** przetwarzania danych ujawniających stan zdrowia, pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, przynależność partyjną lub związkową, dane genetyczne, dane biometryczne, nałogi, preferencje seksualne, chyba że wymagają tego obowiązujące przepisy prawa lub osoba, której dane dotyczą, wyraziła na to pisemną zgodę;
2. Dane o skazaniach, w tym dane o niekaralności można przetwarzać wyłącznie w zakresie uregulowanym w art. 6 ust. 1 pkt 10 ustawy z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz.U. 2017 poz. 678 wraz z późniejszymi zmianami);

§ 18.
**Profilowanie danych osobowych.**

1. Profilowanie polega na automatycznym przetwarzaniu danych osobowych, dopuszczalnym pod warunkiem spełnienia przesłanek określonych przepisami prawa;
2. W przypadku profilowania danych osobowych w związku z działalnością ZUK zabrania się używania danych wymienionych w § 17, chyba, że wymagają tego obowiązujące przepisy prawa, osoba, której dane dotyczą wyraziła na to zgodę, jest to podyktowane ważnym interesem publicznym;
3. Przy profilowaniu danych ZUK, jako Administrator Danych Osobowych, obowiązkowo wdraża środki ochrony praw, wolności i uzasadnionych interesów osoby, której dane dotyczą;
4. O profilowaniu należy informować osobę, której ono dotyczy na etapie zbierania danych, a także na każdy wniosek osoby, której dane dotyczą;
5. Każda osoba, której dane dotyczą, ma prawo wyrażenia sprzeciwu na profilowanie jej danych osobowych, jeżeli uzna, że narusza to jej prawa i wolności.

## § 19.
## Powierzenie przetwarzania danych osobowych.

1. Powierzenie przetwarzania danych osobowych następuje na podstawie umowy powierzenia lub innego aktu prawnego, zawartej w formie pisemnej lub dopuszczalnej prawem formie elektronicznej (oświadczenie złożone drogą elektroniczną lub zapisane na elektronicznym nośniku informacji, określona opcja internetowa). Wzór umowy powierzenia, zgodny z przepisami obowiązującymi w zakresie ochrony danych osobowych stanowi załącznik do PBI;
2. Do przetwarzania powierzonych danych osobowych mogą być dopuszczeni jedynie pracownicy podmiotów współpracujących lub świadczących usługi na rzecz ZUK (procesorów) w zakresie adekwatnym do celu powierzenia;
3. Umowa powierzenia danych osobowych określa przedmiot i czas trwania przetwarzania, zakres, charakter i cel przetwarzania, rodzaj danych osobowych, kategorie osób, których dane dotyczą oraz obowiązki i prawa stron umowy (administratora i procesora);
4. Podmiot, z którym zostaje zawarta umowa powierzenia jest zobowiązany do wdrożenia środków organizacyjnych i technicznych odpowiednich do ryzyk przetwarzania powierzonych danych, prowadzenia rejestru czynności przetwarzania, zgłaszania naruszeń ochrony danych do organu nadzorczego. Szczegółowy zakres praw i obowiązków procesorów określono w dokumencie o nazwie Wymagania w zakresie bezpieczeństwa informacji dla kontrahentów oraz podmiotów współpracujących z ZUK;
5. Administrator Danych Osobowych zobowiązany jest do dokumentowania powierzania tych danych w postaci wykazu umów powierzenia oraz podmiotów, którym powierzono dane osobowe, za każdym razem, gdy takie powierzenie nastąpi. Wzór wykazu podmiotów, którym powierzono dane osobowe stanowi załącznik do PBI;
6. W przypadku, w którym podmiot określony w umowie powierzenia danych osobowych, w zakresie realizacji swoich usług korzysta z pomocy innych podmiotów (podpowierzenie danych), wymagana jest szczegółowa lub ogólna zgoda ADO na przekazanie powierzonych danych, wyrażona w formie pisemnej lub równoważnej jej formie elektronicznej.

## § 20.
## Udostępnianie danych osobowych.

1. Udostępnienie danych osobowych podmiotowi zewnętrznemu może nastąpić wyłącznie w sytuacji, w której ZUK, jako administrator udostępniający dane, oraz administrator danych pozyskujący dane drogą udostępnienia posiadają odpowiednią podstawę prawną w sprawie ww. czynności;
2. ZUK może odmówić udostępnienia danych osobowych w sytuacji, w której spowodowałoby to istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób oraz w sytuacji, w której dane osobowe nie mają istotnego związku ze wskazanymi motywami działania wnioskującego o udostępnienie danych;
3. W przypadku konieczności udostępniania dokumentów i danych w nich zawartych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych;

4. W przypadku, gdy dane osobowe osoby, od której zostały zebrane, są niekompletne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem przepisów prawa lub są zbędne do realizacji celu, dla którego zostały zebrane, ADO lub osoba przez niego upoważniona jest zobowiązana do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

## § 21.
## Obowiązek informacyjny.

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, ZUK jako Administrator Danych Osobowych, jest obowiązany poinformować tę osobę o:
   a) adresie swojej siedziby i pełnej nazwie,
   b) celu i zakresie zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
   c) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej i konsekwencjach niepodania danych,
   d) Inspektorze Ochrony Danych Osobowych oraz danych kontaktowych do IOD (nr tel., e-mail);
   e) prawnie uzasadnionym interesie administratora, jeżeli na tej podstawie odbywać się będzie przetwarzanie danych,
   f) okresie, przez który dane osobowe będą przechowywane lub o kryteriach tego okresu,
   g) profilowaniu danych,
   h) prawach osoby, której dane dotyczą tj. prawie do usunięcia danych, ograniczenia przetwarzania, przenoszenia danych, cofnięcia zgody (gdy osoba, której dane dotyczą wyraża zgodę na przetwarzanie danych);
2. W przypadku pozyskania danych osobowych z innego źródła, niż osoba, której dane dotyczą, ZUK jest zobowiązany poinformować tę osobę, oprócz wymienionych w ust. 1 pkt 1-8, o źródle pozyskania danych oraz uprawnieniach wynikających z przepisów obowiązujących w zakresie ochrony danych osobowych;
3. Obowiązek poinformowania wymieniony w ust. 1 niniejszego paragrafu powinien być wykonany w momencie zbierania danych z wyjątkiem sytuacji, w której przepis innej ustawy zezwala na przetwarzanie danych osobowych lub osoba, której dane dotyczą, posiada już informacje, których udzielenia wymagają przepisy obowiązujące w zakresie ochrony danych osobowych;
4. Obowiązek poinformowania wymieniony w ust. 2 niniejszego paragrafu powinien zostać spełniony bezpośrednio po utrwaleniu zebranych danych, a więc po zapisaniu danych w sposób umożliwiający ich dalsze przetwarzanie.

## § 22.
## Zgoda na przetwarzanie danych osobowych.

1. Zgodnie z art. 4 ust. 11 RODO, zgoda to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, w którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
2. Zgoda na przetwarzanie danych osobowych nie może być domniemana lub dorozumiana ani wynikać z oświadczenia woli o innej treści, tzn. zgoda nie może być zawarta np. w regulaminie, którego zaakceptowanie wiąże się ze zgodą na warunki w nim zawarte;
3. Zgodnie z ust. 32 preambuły RODO, w przypadku pozyskania zgody w formie innej niż pisemna, na ADO ciąży obowiązek udowodnienia, że została ona pozyskana, a niedorozumiana – *„Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny oznaczać zgody"*;
4. Zgoda na przetwarzanie danych osobowych powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, należy pozyskać odrębną zgodę na każdy cel;
5. Zgodnie z ust. 32 preambuły RODO, elektroniczne pytanie o zgodę musi być jasne, zwięzłe i nie zakłócać niepotrzebnie korzystania z usługi, której dotyczy;
6. Zgoda na przetwarzanie danych osobowych może być odwołana w każdym czasie w sposób tak samo prosty i przystępny, w jaki została pozyskana.

## § 23.

1. Zgoda na przetwarzanie danych osobowych nie jest wymagana w przypadku, gdy dane będą przetwarzane:
   a) w związku z zawarciem umowy z osobą, której dane dotyczą,
   b) na podstawie przepisu prawa,
   c) w interesie publicznym,
   d) w prawnie usprawiedliwionym celu administratora danych,
   e) w przypadku żywotnego interesu osoby, której dane dotyczą, gdy pozyskanie zgody jest konieczne, ale niemożliwe.

## § 24.
## Zabezpieczenia danych osobowych.

1. W celu zapewnienia należytej ochrony przetwarzania danych osobowych, w ZUK zastosowano środki zabezpieczające powierzone zbiory danych w postaci zabezpieczeń technicznych i organizacyjnych typu hasła i loginy, zamki, szafy i szafki zamykane na klucz, procedury postępowania, wyznaczone godziny i dni pracy, automatyczne wylogowywanie z systemu, dostęp do określonych zasobów sieci, upoważnienia, rejestry, audyty, przeglądy itp.
2. Pracownicy oraz pozostałe osoby posiadające dostęp do danych osobowych są zobowiązane do przestrzegania zasad zabezpieczania pomieszczeń i urządzeń w strefach stanowiących obszar przetwarzania danych osobowych.

## § 25.
## Zabezpieczenia techniczne.

1. Dokumenty zawierające dane osobowe w formie papierowej, upoważnione osoby przechowują w obszarze przetwarzania danych w zabezpieczonych pomieszczeniach (zamki na klucz);
2. Pomieszczenia, w których przetwarzane są dane osobowe są zabezpieczone przed skutkami pożaru za pomocą instalacji przeciwpożarowej;
3. W przypadku konieczności zniszczenia papierowych dokumentów zawierających dane osobowe, ich zniszczenia dokonuje się poprzez pocięcie w niszczarce;
4. W przypadku wystąpienia konieczności dostępu do zbioru danych osobowych w czasie nieobecności pracownika upoważnionego do przetwarzania danych w tym zbiorze, IOD, w porozumieniu z ASI w zakresie dostępu do systemu informatycznego, może udostępnić ten zbiór innemu pracownikowi w celu dokonania niezbędnych czynności służbowych. Po powrocie nieobecny pracownik otrzymuje nowe indywidualne hasło dostępu;
5. Z każdego zdarzenia opisanego w ust. 3 niniejszego paragrafu, IOD sporządza Raport, w którym podaje: imiona i nazwiska osób zastępujących nieobecnego pracownika;
6. Zastosowany system informatyczny umożliwia rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych;
7. Zastosowany system informatyczny umożliwia określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego w tym systemie zbioru danych osobowych;
8. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

## § 26.
## Zabezpieczenia organizacyjne.

1. Opracowano i wdrożono Politykę Bezpieczeństwa Informacji w ZUK;
2. Wyznaczono ASI, który sprawuje nadzór nad przetwarzaniem danych osobowych w systemie informatycznym;
3. Powołano Inspektora Ochrony Danych Osobowych, który sprawuje nadzór nad zgodnością przetwarzania danych osobowych z obowiązującymi w tym zakresie przepisami oraz realizuje obowiązki opisane w § 8 i 9 niniejszego dokumentu.
4. Wszystkie osoby wykonujące czynności związane z przetwarzaniem danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony tych danych;
5. Wszystkie osoby wykonujące czynności związane z przetwarzaniem danych osobowych w systemie informatycznym (Użytkownicy systemu) zostały przeszkolone w zakresie zasad korzystania i zabezpieczeń tego systemu;
6. Do przetwarzania danych osobowych zostały dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych Osobowych oraz które podpisały oświadczenie o zachowaniu poufności zobowiązujące je do zachowania przetwarzanych danych w tajemnicy;
7. Prowadzone są wykazy osób i podmiotów, którym udostępniono lub powierzono przetwarzanie danych osobowych;

8. Przetwarzanie danych osobowych przez osoby upoważnione odbywa się w wyznaczonych pomieszczeniach, zgodnie z obszarem przetwarzania danych;
9. Dostęp osób nieposiadających stosownych upoważnień do pomieszczeń, w których przetwarzane są dane osobowe odbywa się wyłącznie za zgodą ADO lub w obecności i pod nadzorem osób upoważnionych;
10. Dokumenty zawierające dane osobowe w formie papierowej, upoważnione osoby przechowują w obszarze przetwarzania danych w zabezpieczonych pomieszczeniach (zamki na klucz, karty zbliżeniowe);
11. Wykonane kopie zapasowe zbiorów danych osobowych przechowywane są w pomieszczeniu innym niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.

**§ 27.**

1. Wszyscy pracownicy posiadający dostęp do danych osobowych przed przystąpieniem do pracy uczestniczą w szkoleniu dotyczącym obowiązujących przepisów prawa z zakresu ochrony danych osobowych oraz obowiązujących w ZUK procedur wewnętrznych;
2. Zakres czynności dla osoby upoważnionej do przetwarzania danych osobowych określa jednocześnie zakres odpowiedzialności tej osoby za ochronę przetwarzanych danych osobowych w stopniu adekwatnym do jej zadań na stanowisku pracy;

**§ 28.**

1. Pracownicy ZUK są zobowiązani do informowania IOD o zauważonych próbach nieuprawnionego dostępu do pomieszczeń, o których mowa w ust. 1.

**§ 29.**

1. ADO w porozumieniu z IOD oraz ASI może określić pomieszczenia, do których dostęp osób sprzątających będzie ograniczony i możliwy tylko pod nadzorem osób uprawnionych do przebywania w tych pomieszczeniach;
2. Osoby opuszczające puste pomieszczenie, w którym przetwarzane są dane osobowe, zobowiązane są do zamknięcia drzwi na klucz. Zabrania się pozostawiania klucza w drzwiach po ich zewnętrznej stronie, za wyjątkiem sytuacji związanych z ochroną przeciwpożarową;
3. Zabrania się samowolnego dorabiania kluczy oraz ich wynoszenia poza siedzibę ZUK.
4. Po zakończeniu pracy pracownik zobowiązany jest wylogować się z systemu informatycznego, zamknąć okna w pomieszczeniu, umieścić materiały i dokumenty zawierające dane osobowe w szafach lub szufladach zamykanych na klucz, zgodnie z zasadą czystego biurka, czystej drukarki i czystej kopiarki (o ile takie urządzenia znajdują się w pomieszczeniu) zniszczyć w niszczarce wszystkie materiały zbędne w postaci błędnie utworzonej lub niepotrzebnej dokumentacji mającej krótkotrwałe znaczenie praktyczne, m.in. wydruków komputerowych i innych materiałów analogowych zawierających dane osobowe;

§ 30.

1. Udostępnianie drogą pocztową lub kurierską dokumentów i materiałów zawierających dane osobowe może odbywać się przesyłką rejestrowaną, a w przypadku danych zawartych na nośnikach magnetycznych, optycznych lub elektronicznych – przesyłką rejestrowaną za potwierdzeniem odbioru;
2. W ZUK dopuszcza się stosowanie zabezpieczeń organizacyjnych i technicznych innych, niż wymienione w § 22-27.

§ 31.
**Sprawdzenia.**

1. Sprawdzenia zgodności przetwarzania danych osobowych z przepisami prawa oraz wewnętrznymi regulacjami obowiązującymi w tym zakresie w ZUK dokonuje IOD (IOD) we współpracy z ASI w zakresie sprawdzeń dotyczących przetwarzania danych osobowych w systemie informatycznym. Odbiorcą sprawdzeń jest Administrator Danych Osobowych lub w określonych przypadkach organ nadzorczy;
2. W przypadku otrzymania informacji o naruszeniu bezpieczeństwa danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia, IOD przeprowadza niezwłocznie sprawdzenie doraźne;
3. Sprawdzeniu podlega system informatyczny, w którym przetwarzane są dane osobowe, zabezpieczenia fizyczne i organizacyjne, bezpieczeństwo osobowe oraz zgodność stanu faktycznego z wymaganiami prawnymi;
4. IOD przygotowuje plan sprawdzeń na okres nie krótszy niż kwartał i nie dłuższy niż rok. Plan obejmuje, co najmniej jedno sprawdzenie i jest przedstawiany ADO nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu nim objętego;
5. Zbiory danych oraz system informatyczny służący do przetwarzania lub zabezpieczania danych osobowych są obejmowane sprawdzeniem, co najmniej raz na pięć lat;
6. Dokumentowanie przez IOD czynności w toku sprawdzenia polega na tworzeniu materiałów w postaci papierowej lub elektronicznej w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych i opracowania sprawozdania;
7. Po zakończeniu sprawdzenia IOD przygotowuje sprawozdanie, zgodnie z wytycznymi określnymi w obowiązujących przepisach prawa w zakresie ochrony danych osobowych, które zawiera opis ustalonego stanu faktycznego podlegającego ocenie oraz analizę w zakresie przestrzegania przepisów o ochronie danych osobowych w odniesieniu do ustalonego stanu faktycznego. W sprawozdaniu IOD stwierdza, czy naruszone zostały przepisy o ochronie danych osobowych, a jeżeli tak, to jakie są planowane lub podjęte działania przywracające stan zgodny z prawem. Sprawozdanie jest sporządzane w postaci elektronicznej albo w postaci papierowej.
8. IOD przekazuje sprawozdanie ze sprawdzenia planowego do ADO nie później niż w terminie 30 dni od zakończenia sprawdzenia. Sprawozdanie ze sprawdzenia doraźnego przekazywane jest niezwłocznie po zakończeniu sprawdzenia.

## § 32.
## Odpowiedzialność.

1. Za zapewnienie pracownikom warunków organizacyjnych i technicznych mających na celu zapewnienie należytego bezpieczeństwa danych osobowych odpowiada Administrator Danych Osobowych w porozumieniu z osobami odpowiedzialnymi za poszczególne komórki organizacyjne ZUK;
2. IOD w porozumieniu z ASI oraz osobami odpowiedzialnymi za poszczególne komórki organizacyjne ZUK odpowiada za zapewnienie bieżącej edukacji pracowników dotyczącej zasad bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym i systemie tradycyjnym oraz wnioskuje do ADO o szkolenia w tym zakresie;
3. Na pracownikach oraz osobach upoważnionych do przetwarzania danych osobowych, w zakresie ich uprawnień i odpowiedzialności, ciąży obowiązek dbałości o zabezpieczanie danych osobowych przed ich udostępnieniem, zabraniem, przetwarzaniem z naruszeniem przepisów prawa przez osoby nieuprawnione oraz zmianą, uszkodzeniem, utratą lub zniszczeniem.

## § 33.

1. Nieprzestrzeganie zasad ochrony danych osobowych grozi odpowiedzialnością karną wynikającą z przepisów obowiązujących w zakresie ochrony danych osobowych;
2. Odpowiedzialności karnej podlega każda osoba w ZUK , która:
   a) przetwarza w zbiorze danych dane osobowe, do których nie jest upoważniona,
   b) przetwarza w zbiorze danych dane, których przetwarzanie jest zabronione,
   c) przetwarza w zbiorze danych dane niezgodne z celem stworzenia tego lub innych zbiorów,
   d) udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym,
   e) nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o przysługujących jej prawach,
   f) uniemożliwia osobie, której dane dotyczą, korzystanie z przysługujących jej praw;
3. Złamanie zasad Polityki Bezpieczeństwa Informacji stanowi incydent, o którym powinien być niezwłocznie powiadomiony IOD. O podjęciu działań naprawczych decyduje ADO na podstawie projektu działań opracowanego przez IOD. W przypadku wystąpienia incydentu związanego z przetwarzaniem danych osobowych w systemie informatycznym, projekt naprawczy opracowuje i przedstawia także ASI.
4. Łamanie zasad wynikających z niniejszej PBI może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych i może skutkować nałożeniem kary porządkowej na zasadach określonych w przepisach prawa pracy oraz procedurach wewnętrznych, w szczególności w przypadku osoby, która po stwierdzeniu naruszenia bezpieczeństwa danych osobowych lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym fakcie IOD;
5. Udokumentowane umyślne złamanie zasad określonych w PBI jest traktowane jako ciężkie naruszenie obowiązków pracowniczych uzasadniające rozwiązanie stosunku pracy bez wypowiedzenia z winy pracownika.

## Rozdział 4.
## Ogólne warunki korzystania z systemu informatycznego. Konfiguracja sprzętu informatycznego użytkownika systemu. Procedury nadawania uprawnień. Poczta elektroniczna. Procedury niszczenia nośników danych.

### § 34.
### Zasady korzystania z systemu informatycznego.

1. Podstawowym celem zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych jest zapewnienie jak najwyższego standardu bezpieczeństwa tych danych. Priorytetowe jest zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania, charakteru poufnego wraz z zachowaniem ich integralności oraz integralności systemów informatycznych stosowanych w ZUK ;
2. Istotnym elementem osiągnięcia celu, o którym mowa w ust. 1 jest zapewnienie odpowiedniego poziomu kontroli dostępu:
   a) do sieci, w tym urządzeń serwerowych,
   b) do systemów operacyjnych,
   c) do aplikacji,
   d) do informacji i zbiorów danych, wraz z określeniem trybu dostępu.
3. Zasady zachowania bezpieczeństwa w systemie informatycznym obejmują wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę informacji przed ich nieuprawnionym przetwarzaniem;
4. Każdy Użytkownik systemu informatycznego stosowanego w ZUK jest zobowiązany do zapoznania się z zasadami korzystania z tego systemu;
5. Ze względu na fakt, że użytkowane w ZUK programy informatyczne służące do przetwarzania danych osobowych są połączone z siecią Internet, wprowadza się **wysoki poziom bezpieczeństwa**;
6. Korzystanie z funkcjonalności systemu informatycznego jest możliwe pod warunkiem nadania przez ASI uprawnień Użytkownika systemu informatycznego;
7. Szczegółowe procedury nadawania uprawnień do systemu informatycznego reguluje Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w ZUK.

### § 35.

1. Zgodnie z postanowieniami niniejszej PBI, zabrania się Użytkownikowi systemu informatycznego podejmowania jakichkolwiek czynności mających na celu naruszenie bezpieczeństwa przetwarzanych danych, w tym prób przełamania zabezpieczeń tego systemu;
2. W celu zapobieżenia nieautoryzowanemu dostępowi do systemu informatycznego Użytkownik nie może przechowywać danych służących do logowania do systemu w miejscach dostępnych dla innych osób oraz ujawniać danych służących do logowania innym osobom;
3. Zabronione jest korzystanie z systemu informatycznego z użyciem danych dostępowych innego Użytkownika;

4. Użytkownicy są zobowiązani do ustawienia ekranów monitorów w taki sposób, aby uniemożliwić osobom postronnym wgląd lub spisanie informacji aktualnie wyświetlanej na ekranie monitora;
5. Użytkownik zobowiązany jest do przestrzegania zasady „czystego biurka", w szczególności przed opuszczeniem swego stanowiska pracy powinien schować wszelkie informatyczne nośniki danych;
6. W czasie kopiowania, drukowania dokumentów zawierających dane osobowe, Użytkownik zobowiązany jest do zachowania zasady „czystej drukarki", „czystej kopiarki", w szczególności przed opuszczeniem stanowiska kopiowania/drukowania upewnić się, że w urządzeniach nie pozostały dokumenty zawierające dane osobowe;
7. Przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych z użyciem urządzeń mobilnych. Użytkownik jest zobowiązany do sprawdzenia, czy posiadane przez niego dane są należycie zabezpieczone przed dostępem osób nieupoważnionych;
8. Po zakończeniu przetwarzania danych osobowych, Użytkownik zobowiązany jest do należytego zabezpieczenia ich przed dostępem osób nieupoważnionych

**§ 36.**
**Konfiguracja sprzętu komputerowego Użytkownika systemu.**

1. System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych oraz logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem, w tym kontroli przepływu informacji pomiędzy system a siecią publiczną oraz kontrolę działań inicjowanych z sieci publicznej i systemu;
1. Każdy dostęp do danych osobowych jest zarejestrowany;
2. Urządzenie mobilne (laptop, tablet itp.) zawierające dane osobowe jest zabezpieczone przed nieuprawnionym dostępem;
3. Minimalne środki ochrony to:
   a) zainstalowanie na stacjach oprogramowania antywirusowego wraz z konfiguracją zapory internetowej „firewall" używanego systemu operacyjnego;
   b) wdrożenie systemu aktualizacji systemu operacyjnego oraz jego składników,
   c) wymaganie podania hasła przed uzyskaniem dostępu do systemu operacyjnego,
   d) niepozostawianie niezablokowanych stacji roboczej bez nadzoru,
   e) praca z wykorzystaniem konta nieposiadającego uprawnień administracyjnych.
4. Użytkownik jest zobowiązany do stałego monitorowania komunikatów pochodzących z oprogramowania antywirusowego zainstalowanego na stacji roboczej oraz na urządzeniach mobilnych i reagowania na nie;
5. W przypadku niesprawdzenia przez Użytkownika systemu pliku dostarczonego z zewnątrz, oprogramowanie antywirusowe automatycznie chroni system poprzez monitorowanie plików w stanie rzeczywistym. W przypadku wykrycia zagrożenia, oprogramowanie stosownie reaguje na to zagrożenie
6. Wygaszacze ekranu systemowo ustawiane są na aktywację po 10 minutach bezczynności na danej stacji roboczej oraz w razie potrzeby (np. opuszczenie miejsca przetwarzania danych) skrótem klawiaturowym;
7. Uruchomienie wygaszacza ekranu wiąże się z koniecznością ponownego zalogowania, celem wznowienia pracy stacji roboczej.

## § 37.
## Procedury nadawania uprawnień.

1. Dostęp do systemu informatycznego służącego do przetwarzana danych osobowych może uzyskać wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych nadane przez ADO (załącznik PBI), która podpisała oświadczenie o zachowaniu poufności (załącznik do PBI);
2. Uprawnienia dostępu do systemu informatycznego służącego do przetwarzania danych osobowych nadaje ASI na wniosek osoby odpowiedzialnej za daną komórkę organizacyjną ZUK;
3. Uprawnienia, o których mowa w ust. 2 określają poziom dostępu do sieci, w tym urządzeń serwerowych, do systemów operacyjnych, do aplikacji i informacji;
4. Po nadaniu uprawnień w systemie informatycznym, ASI przydziela Użytkownikowi login i hasło tymczasowe. Hasło tymczasowe Użytkownik zmienia na własne przy pierwszym logowaniu;
5. Hasło Użytkownika musi się składać co najmniej z 8 znaków, w tym zawierać małe i wielkie litery oraz cyfry lub znaki specjalne, nie może zawierać znaków następujących po sobie na klawiaturze bądź tych samych liter lub cyfr, nie może zawierać imion, nazwisk, przezwisk, inicjałów, dat, numerów rejestracyjnych samochodów, numerów telefonów i innych kombinacji znaków mogących doprowadzić do łatwego rozszyfrowania go przez osoby nieupoważnione, nie może być zapisywane w systemie w postaci jawnej, nie może być wyświetlane na ekranie komputera w sposób jawny, nie może być ujawnione innej osobie, nawet po utracie ważności, musi być zabezpieczone przez Użytkownika przed nieuprawnionym dostępem osób trzecich;
6. W przypadku zapomnienia przez Użytkownika konstrukcji hasła, winien on niezwłocznie zawiadomić ASI, który nadaje nowe hasło, postępując zgodnie z procedurą obowiązującą przy nadawaniu uprawnień dostępu do systemu informatycznego;
7. ASI dokonuje rejestracji i prowadzi wykaz loginów przydzielonych poszczególnym Użytkownikom, który wiąże loginy z imiennie wskazanymi osobami;
8. Użytkownikom nadawane są uprawnienia do prac tylko w modułach i funkcjach programu wymaganych dla realizacji powierzonych im zadań;
9. Użytkownik systemu informatycznego ponosi odpowiedzialność za bezpieczeństwo danych osobowych przetwarzanych we wszystkich operacjach wykonanych przy użyciu jego loginu i hasła dostępu;
10. W przypadku wygaśnięcia przesłanek uprawniających Użytkownika do przetwarzania danych osobowych, w szczególności cofnięcia upoważnienia do ich przetwarzania, ASI przy współpracy z IOD zobowiązany jest do wyrejestrowania Użytkownika z systemu informatycznego, do którego był uprawniony;
11. Wyrejestrowanie Użytkownika z ewidencji osób upoważnionych do przetwarzania informacji następuje poprzez zablokowanie go we wszystkich opcjach systemu informatycznego, do których miał dostęp.

## § 38.
## Poczta elektroniczna.

1. Użytkownik zobowiązany jest do dbania o bezpieczeństwo poczty elektronicznej, w szczególności do używania silnego hasła dostępu, nieotwierania załączników do poczty i linków pochodzących z nieznanych źródeł oraz zachowania ostrożności podczas otwierania nieoczekiwanych załączników w korespondencji pochodzącej od znanych nadawców.
2. Szczegółowe zasady korzystania z poczty elektronicznej reguluje Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w ZUK.

## § 39.
## Procedura niszczenia danych na nośnikach elektronicznych.

1. W odniesieniu do nośników przenośnych (pendrive) oraz nośników danych zainstalowanych w komponentach informatycznych – złomowanych stosowane są mechanizmy bezpiecznego kasowania informacji:
   a) za pomocą specjalistycznego oprogramowania,
   b) przy użyciu demagnetyzacji,
   c) poprzez fizyczne niszczenie (pocięcie, spalenie) nośników;
2. ASI dokonuje kontroli prawidłowości usunięcia informacji;
3. Nośniki elektroniczne, które nie mogą być ponownie wykorzystane, są niszczone mechanicznie lub oddawane do utylizacji przez firmę specjalistyczną;
4. Za właściwe skasowanie informacji zawartej na nośniku przenośnym lub w pamięci masowej stacji roboczej odpowiada Użytkownik;
5. Za kasowanie informacji z pamięci masowych serwerów oraz nośników kopii archiwalnych i zapasowych odpowiada ASI;
6. Niszczenie nośnika zostaje odnotowane w protokole zniszczenia (załącznik do PBI)

# Rozdział 5.
# Postępowanie na wypadek zagrożenia bezpieczeństwa danych osobowych.

## § 40.

1. Ryzyko w zakresie bezpieczeństwa informacji, w tym danych osobowych, definiuje się jako prawdopodobieństwo wystąpienia zagrożeń i powstanie szkód, zniszczeń oraz przerw lub zakłóceń prawidłowego funkcjonowania systemu tradycyjnego oraz systemu informatycznego, w których przetwarzane są dane osobowe;
2. Zarządzanie ryzykiem jest procesem identyfikacji zasobów, odpowiadających im podatności i zagrożeń, oceny prawdopodobieństwa ich wystąpienia, wielkości potencjalnych strat oraz przeciwdziałania i określenia kryteriów akceptowalności ryzyka;
3. Zarządzanie ryzykiem obejmuje możliwie jak najszybszą identyfikację ryzyka związanego z planowanym działaniem, ocenę stopnia wpływu ryzyka na uzyskane wyniki lub cele oraz zastosowanie odpowiednich środków kontroli ryzyka;

4. Proces zarządzania ryzykiem w zakresie bezpieczeństwa informacji zawierających dane osobowe, odnoszącym się do działalności ZUK, dokonywany jest przez IOD we współpracy z osobami odpowiedzialnymi za poszczególne komórki organizacyjne oraz z ASI w zakresie systemu informatycznego;
5. Pracownicy, do których przypisano poszczególne ryzyka (właściciele ryzyka), określają prawdopodobieństwo wystąpienia zidentyfikowanych ryzyk oraz ich skutek i wpływ na realizowane zadania z jednoczesnym wskazaniem istniejących mechanizmów kontroli i propozycją reakcji na ryzyko;
6. IOD w porozumieniu z ASI w przypadku ryzyk dotyczących bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym, opracowuje roczne sprawozdania, które w postaci raportu o zidentyfikowanych ryzykach przekazuje ADO.

**§ 41.**

1. Niezależnie od corocznej oceny ryzyka, Administrator Danych Osobowych na podstawie informacji od IOD dokonuje ich oceny po każdorazowym wystąpieniu incydentu oraz każdorazowej zmianie mogącej wpływać na poziom ryzyka, w tym szczególnie zmianie struktury organizacyjnej, otoczenia dotyczącego realizacji umów z nowymi podmiotami, technologii, infrastruktury, pracowników, metod pracy, przepisów prawa;
2. Niezwłocznie po wystąpieniu incydentu, IOD przedstawia ADO do oceny zidentyfikowane ryzyka oraz propozycje działań korygujących i zapobiegawczych;
3. Na podstawie raportów i sprawozdań otrzymanych od IOD, ADO podejmuje ostateczną decyzję w zakresie realizacji działań zapewniających ochronę przetwarzanych informacji;
4. Do działań ADO wskazanych w ust. 3 należy w szczególności:
   a) zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia,
   b) utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację,
   c) przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy,
   d) podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji,
   e) dokonanie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4,
   f) zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich,

g) zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez monitorowanie dostępu do informacji, czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji,
h) ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość,
i) zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie,
j) zawieranie w umowach serwisowych zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji,
k) ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych,
l) zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
   - dbałości o aktualizację systemu operacyjnego,
   - minimalizowaniu ryzyka utraty informacji w wyniku awarii,
   - ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
   - stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
   - zapewnieniu bezpieczeństwa plików systemowych,
   - redukcji ryzyka wynikającego z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
   - niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
   - kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i PBI,
m) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w sposób, umożliwiający szybkie podjęcie działań korygujących,
n) zapewnienie okresowego audytu wewnętrznego lub zewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

**§ 42.**

1. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:

a) próby naruszenia ochrony danych:
   - z zewnątrz - włamania do systemu, podsłuch, kradzież danych
   - z wewnątrz - nieumyślna lub celowa modyfikacja danych, kradzież danych,
b) programy destrukcyjne: wirusy, konie trojańskie, makra, bomby logiczne,
c) awarie sprzętu lub uszkodzenie oprogramowania,
d) zabór sprzętu lub nośników z ważnymi danymi ,
e) inne skutkujące utratą danych osobowych, bądź wejściem w ich posiadanie osób nieuprawnionych,
f) usiłowanie zakłócenia działania systemu informatycznego;

2. Do typowych incydentów zagrażających bezpieczeństwu danych osobowych należą:
   a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   b) niewłaściwe zabezpieczenie sprzętu IT i oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
   c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek),
   d) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasiania, utrata łączności),
   e) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych),
   f) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania);
3. Do typowych źródeł informacji o incydentach, zagrożeniach lub słabościach systemu zalicza się:
   a) zgłoszenia od Użytkowników,
   b) alarmy z systemów informatycznych,
   c) analizy incydentów,
   d) wyniki audytów / kontroli.

**§ 43.**

Każda osoba posiadająca dostęp do danych osobowych, w przypadku stwierdzenia zagrożenia lub naruszenia ochrony tych danych, zobowiązana jest poinformować Administratora Bezpieczeństwa Informacji / IOD lub ASI w sytuacjach dotyczących użytkowania systemu informatycznego. Zasady działania w takich przypadkach określa **tabela nr 1:**

Tabela nr 1. Zasady działania w przypadku zagrożenia bezpieczeństwa danych osobowych

| Kod uchybienia lub zagrożenia | Uchybienie i zagrożenie nieświadome wewnętrzne i zewnętrzne | Postępowanie w przypadku uchybienia lub zagrożenia |
|---|---|---|
| **W zakresie pomieszczeń i infrastruktury służących do przetwarzania danych osobowych** | | |
| A1 | Pomieszczenie, w którym przechowywane są dane osobowe pozostaje bez nadzoru | Należy zabezpieczyć dane osobowe oraz powiadomić IOD, który powiadamia ADO. IOD sporządza Protokół uchybienia. |
| A2 | Dostęp do danych mają osoby nieupoważnione | Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić IOD, który powiadamia ADO i sporządza Protokół uchybienia. |
| A3 | Próba kradzieży danych osobowych w formie papierowej | Należy nie dopuścić do kradzieży danych osobowych i powiadomić IOD, który powinien zabezpieczyć dane i powiadomić ADO. IOD, powiadamia ADO i sporządza Protokół zagrożenia. |
| A4 | Nieuprawniony dostęp do danych osobowych w formie papierowej | Należy uniemożliwić dostęp osób bez upoważnienia oraz powiadomić IOD, który sporządza Protokół uchybienia i powiadamia ADO. |
| A5 | Dane osobowe przechowywane są w niezabezpieczonym pomieszczeniu | Należy powiadomić IOD, który powinien zabezpieczyć pomieszczenie, powiadomić ADO i sporządzić Protokół uchybienia. |
| A6 | Próba włamania do pomieszczenia/budynku | Należy zabezpieczyć dowody i powiadomić IOD, który sprawdza stan uszkodzeń, zabezpiecza dowody i wzywa policję. IOD, powiadamia ADO i sporządza protokół zagrożenia. |
| A7 | Zniszczenie lub modyfikacja danych osobowych w formie papierowej | Należy zabezpieczyć dowody i powiadomić IOD, który sprawdza stan uszkodzeń, zabezpiecza dowody, powiadamia ADO oraz sporządza protokół zagrożenia. |
| A8 | Wyrzucenie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie | Należy zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić IOD oraz przełożonych. IOD, sporządza Protokół zagrożenia. |
| **W zakresie przetwarzania danych osobowych w systemie informatycznym** | | |
| B1 | Komputer nie jest zabezpieczony hasłem | Należy zabezpieczyć dane osobowe oraz powiadomić ASI i IOD, który powiadamia ADO i sporządza Protokół uchybienia. |
| B2 | Nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym | Należy powiadomić ASI i IOD, który we współpracy z ASI powinien sprawdzić system uwierzytelniania oraz sprawdzić, czy nie doszło do kradzieży lub zniszczenia danych. Na podstawie informacji uzyskanych od ASI, IOD powiadamia ADO i sporządza Protokół uchybienia. |
| B3 | Próba kradzieży danych osobowych poprzez zewnętrzny nośnik danych | Należy nie dopuścić do kradzieży danych i powiadomić IOD i ASI. ASI w porozumieniu z IOD, powinien zabezpieczyć nośnik danych i powiadomić ADO. IOD, sporządza Protokół zagrożenia. |
| B4 | Działanie zewnętrznych aplikacji, wirusów, złośliwego oprogramowania | Należy zawiadomić ASI i IOD. ASI powinien przeprowadzić audyt systemów zabezpieczeń, a w szczególności systemów antywirusowych i firewall. ASI przekazuje wynik audytu IOD, który powinien ocenić, czy nie doszło do utraty danych osobowych i w zależności od tego sporządzić protokół uchybienia lub zagrożenia. IOD powiadamia ADO. |
| B11 | Brak aktywnego oprogramowania antywirusowego | Należy powiadomić ASI. ASI powinien zaktualizować lub nabyć oprogramowanie antywirusowe i powiadomić IOD, który powiadamia ADO i sporządza Protokół uchybienia. |
| B13 | Zniszczenie lub modyfikacja danych osobowych w systemie informatycznym | Należy zabezpieczyć dowody i powiadomić ASI. ASI sprawdza stan uszkodzeń, zabezpiecza dowody i powiadamia IOD, który powiadamia ADO i sporządza Protokół zagrożenia. |
| B14 | Uszkodzenie komputerów, nośników danych | Należy powiadomić IOD, który w porozumieniu z ASI powinien ocenić w wyniku czego doszło do zniszczenia i przywrócić dane z kopii zapasowej. IOD powiadamia ADO i sporządza Protokół zagrożenia. |
| B15 | Próba nieprawidłowej interwencji przy sprzęcie komputerowym | Należy uniemożliwić dostęp osób do sprzętu komputerowego oraz powiadomić ASI, który powiadamia IOD, który powiadamia ADO i sporządza Protokół uchybienia. |
| **W zakresie zdarzeń niezależnych od działalności człowieka** | | |
| C16 | Zdarzenia losowe (powódź, pożar, zalanie itp.) | IOD powoduje oszacowanie strat, powiadamia ADO i sporządza Protokół zagrożenia lub uchybienia. |

## § 44.

1. W przypadku stwierdzenia wystąpienia zagrożenia, IOD prowadzi postępowanie wyjaśniające, w toku którego ustala zakres i przyczyny zagrożenia oraz jego potencjalne skutki, inicjuje ewentualne działania dyscyplinarne, rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości, dokumentuje prowadzone postępowania;
2. W przypadku stwierdzenia incydentów naruszenia bezpieczeństwa danych osobowych IOD prowadzi postępowanie wyjaśniające, w toku którego:
   a) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały i zabezpiecza ewentualne dowody oraz podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),
   b) ustala osoby odpowiedzialne za naruszenie,
   c) inicjuje działania dyscyplinarne, wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,
   d) dokumentuje prowadzone postępowania;
3. IOD jest odpowiedzialny za analizę incydentów naruszenia bezpieczeństwa, zagrożeń lub słabości systemu ochrony danych osobowych. Gdy stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych, określa źródło powstania incydentu, zagrożenia lub słabości, zakres działań korygujących lub zapobiegawczych, termin realizacji oraz osobę odpowiedzialną;
4. IOD jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych. Po przeprowadzeniu działań korygujących lub zapobiegawczych, jest zobowiązany do oceny efektywności ich zastosowania i prowadzenia stosownej dokumentacji.

# Rozdział 6.
# Postanowienia końcowe.

## § 45.

1. W sprawach nieuregulowanych niniejszym dokumentem, znajdują zastosowanie przepisy obowiązujące w zakresie ochrony danych osobowych;
2. Nad aktualnością Polityki Bezpieczeństwa Informacji w ZUK czuwa Inspektor Ochrony Danych Osobowych we współpracy z ASI w zakresie przetwarzania danych osobowych w systemie informatycznym.

Załącznik Nr 2
do Zarządzenia
Dyrektora
Nr 02/2022
z dnia 12.10.2022

# Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Zakładzie Usług Komunalnych w Węglińcu ul. Partyzantów 8 Węgliniec, 59-940 Węgliniec

*Zatwierdzam do stosowania*

DYREKTOR
Zakładu Usług Komunalnych w Węglińcu
mgr inż. Krzysztof Polewski

## SPIS TREŚCI

## Rozdział 1.
## Postanowienia ogólne.

### § 1.
### Podstawy prawne.

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO) (Dz. Urz. UE L119 z 4 maja 2016 r.);

### § 2.
### Słownik pojęć.

1. **Administrator Danych Osobowych** (**ADO**) - organ, jednostka organizacyjna, podmiot lub osoba decydujące o celach i środkach przetwarzania danych osobowych. W tym przypadku Administratorem Danych Osobowych jest Zakład Usług Komunalnych w Węglińcu, ul. Partyzantów, 59-940 Węgliniec reprezentowany przez Dyrektora.
2. **Inspektor Ochrony Danych Osobowych (IOD)** - osoba fizyczna upoważniona przez Administratora Danych Osobowych, zajmująca się zapewnianiem przestrzegania przepisów o ochronie danych osobowych oraz prowadzeniem wymaganej prawem dokumentacji związanej z przetwarzaniem tych danych przez administratora;
3. **Administrator Systemów Informatycznych (ASI)** – osoba fizyczna wyznaczona przez Administratora Danych Osobowych, zajmująca się sprawowaniem ogólnego nadzoru nad bezpieczeństwem organizacyjnym, fizycznym oraz technicznym danych osobowych przetwarzanych w systemie informatycznym.
4. **Baza danych osobowych** – zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci wewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze – rekordów lub obiektów, w których są zapisywane dane osobowe;
5. **ZUK** – Zakład Usług Komunalnych w Węglińcu, ul. Partyzantów 8, 59-940 Węgliniec.
6. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, uwierzytelniający osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
7. **Identyfikator / login** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
8. **IZSI / Instrukcja** – niniejszy dokument;
9. **Kopia pełna** - kopia zapasowa całości danych osobowych przetwarzanych w systemie informatycznym;
10. **Niezgodność** - niespełnienie wymagania, czyli potrzeby lub oczekiwania, które zostało ustalone, przyjęte zwyczajowo lub jest obowiązkowe
11. **Elektroniczne nośniki danych** – przedmioty fizyczne, na których możliwe jest zapisanie informacji w celu ich przechowywania, przetwarzania i transmisji. Każdy nośnik danych charakteryzuje określona gęstość zapisu, wynikająca z jego właściwości fizycznych;
12. **Polityka Bezpieczeństwa Informacji (PBI)** – przyjęty do stosowania dokument Polityka Bezpieczeństwa Informacji w ZUK;

13. **Przetwarzane danych** – wszelkie operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te operacje, które wykonuje się w systemie informatycznym;
14. **Raport** – przygotowane przez system informatyczny zestawienie zakresu i treści przetwarzanych danych;
15. **System informatyczny (system IT)** - zespół współpracujących ze sobą urządzeń, programów, systemów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
16. **Serwisant** – pracownik firmy zewnętrznej lub pracownik administratora zajmujący się instalacją, naprawą i konserwacją sprzętu komputerowego;
17. **Sieć publiczna** – sieć telekomunikacyjna wykorzystywana głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych;
18. **Teletransmisja** – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej
19. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
20. **Użytkownik** - wyznaczony do przetwarzania danych osobowych pracownik, który odbył stosowne szkolenie w zakresie ochrony tych danych oraz uzyskał upoważnienie i uprawnienia dostępu do systemu informatycznego służącego do przetwarzania danych osobowych;
21. **Zabezpieczenie danych w systemie informatycznym** - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

## § 3.
## Cel i zakres stosowania instrukcji.

1. Podstawowym celem zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych jest zapewnienie jak najwyższego standardu bezpieczeństwa tych danych. Priorytetowe jest zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania, charakteru poufnego wraz z zachowaniem ich integralności oraz integralności systemów informatycznych stosowanych w ZUK;
2. Istotnym elementem osiągnięcia celu, o którym mowa w ust. 1 jest zapewnienie odpowiedniego poziomu oraz kontroli dostępu:
   a) do sieci, w tym urządzeń serwerowych,
   b) do systemów operacyjnych,
   c) do aplikacji,
   d) do informacji i zbiorów danych, wraz z określeniem trybu dostępu.

## § 4.

1. Instrukcja została opracowana zgodnie z Rozporządzeniem 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);
2. Zgodnie z rozporządzeniem wymienionym w ust. 1, uwzględniając fakt, że użytkowane w Ośrodku programy informatyczne służące do przetwarzania danych osobowych są połączone z siecią Internet, wprowadza się **wysoki poziom bezpieczeństwa.**

## § 5.
## Konfiguracja sprzętu komputerowego użytkownika systemu.

1. System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych oraz logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem, w tym kontroli przepływu informacji pomiędzy system a siecią publiczną oraz kontrolę działań inicjowanych z sieci publicznej i systemu;
2. Każdy dostęp do danych osobowych jest zarejestrowany;
3. Urządzenie mobilne (laptop, tablet itp.) zawierające dane osobowe jest zabezpieczone przed nieuprawnionym dostępem;
4. Minimalne środki ochrony to:
   a) zainstalowanie na stacjach zapory sieciowej firewall i oprogramowania antywirusowego,
   b) wdrożenie systemu aktualizacji systemu operacyjnego oraz jego składników,
   c) wymaganie podania hasła przed uzyskaniem dostępu do systemu operacyjnego,
   d) niepozostawianie niezablokowanych stacji roboczej bez nadzoru,
   e) praca z wykorzystaniem konta nieposiadającego uprawnień administracyjnych.

## § 6.

1. Użytkownik jest zobowiązany do stałego monitorowania komunikatów pochodzących z oprogramowania antywirusowego zainstalowanego na stacji roboczej oraz na urządzeniach mobilnych i reagowania na nie;
2. W przypadku niesprawdzenia przez Użytkownika systemu pliku dostarczonego z zewnątrz, oprogramowanie antywirusowe automatycznie chroni system poprzez monitorowanie plików w stanie rzeczywistym. W przypadku wykrycia zagrożenia, oprogramowanie stosownie reaguje na to zagrożenie.

## Rozdział 2.
## Procedury nadawania uprawnień. Metody i środki uwierzytelniania. Wygaszacze ekranu.

### § 7.
### Procedury nadawania uprawnień.

1. Dostęp do systemu informatycznego służącego do przetwarzana danych osobowych może uzyskać wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych nadane przez ADO (załącznik do PBI), która podpisała oświadczenie o zachowaniu poufności (załącznik PBI);
2. Uprawnienia dostępu do systemu informatycznego służącego do przetwarzania danych osobowych nadaje ASI na wniosek osoby odpowiedzialnej za daną komórkę organizacyjną ZUK;
3. Uprawnienia, o których mowa w ust. 2 określają poziom dostępu do sieci, w tym urządzeń serwerowych, do systemów operacyjnych, do aplikacji i informacji;
4. ASI jest zobowiązany upoważnić co najmniej jednego pracownika obsługującego system informatyczny do rejestracji Użytkowników w tym systemie w czasie swojej nieobecności.

### § 8.

1. Po nadaniu uprawnień w systemie informatycznym, ASI przydziela Użytkownikowi login i hasło tymczasowe;
2. Po otrzymaniu hasła tymczasowego Użytkownik ma obowiązek niezwłocznego zalogowania się do systemu informatycznego przy użyciu tego hasła oraz jego zmiany na hasło osobiste;
3. 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;
4. ASI dokonuje rejestracji i prowadzi wykaz loginów przydzielonych poszczególnym Użytkownikom, który wiąże loginy z imiennie wskazanymi pracownikami;
5. Użytkownikom nadawane są uprawnienia do prac tylko w modułach i funkcjach programu wymaganych dla realizacji powierzonych im zadań;
6. Użytkownik systemu informatycznego ponosi odpowiedzialność za bezpieczeństwo danych osobowych przetwarzanych we wszystkich operacjach wykonanych przy użyciu jego loginu i hasła dostępu;
7. W przypadku wygaśnięcia przesłanek uprawniających Użytkownika do przetwarzania danych osobowych, w szczególności cofnięcia upoważnienia do ich przetwarzania, ASI przy współpracy z IOD zobowiązany jest do wyrejestrowania Użytkownika z systemu informatycznego, do którego był uprawniony;
8. Wyrejestrowanie Użytkownika z ewidencji osób upoważnionych do przetwarzania informacji następuje poprzez zablokowanie go we wszystkich opcjach systemu informatycznego, do których miał dostęp.

## § 9.
## Metody oraz środki uwierzytelniania,

1. Dostęp do danych osobowych przetwarzanych w systemie informatycznym odbywa się na podstawie uwierzytelnienia, poprzez podanie indywidualnej nazwy (identyfikatora/loginu) i hasła Użytkownika;
2. Celem stosowania identyfikatora (loginu) Użytkownika jest jednoznaczne określenie osoby, która się nim posługuje;
3. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika, ASI za zgodą IOD nadaje inny identyfikator, odstępując od zasady określonej w ust. 2;
4. W przypadku zmiany imienia lub nazwiska pozostaje pierwotnie nadany identyfikator;
5. Identyfikator Użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie;
6. System informatyczny, w którym przetwarzane są dane osobowe automatycznie wymusza podanie identyfikatora i hasła Użytkownika;

## § 10.

1. Hasło Użytkownika:
   a) musi się składać co najmniej z 8 znaków, w tym zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,
   b) nie może zawierać znaków następujących po sobie na klawiaturze bądź tych samych liter lub cyfr,
   c) nie może zawierać imion, nazwisk, przezwisk, inicjałów, dat, numerów rejestracyjnych samochodów, numerów telefonów i innych kombinacji znaków mogących doprowadzić do łatwego rozszyfrowania go przez osoby nieupoważnione,
   d) nie może być zapisywane w systemie w postaci jawnej,
   e) nie może być wyświetlane na ekranie komputera w sposób jawny,
   f) nie może być ujawnione innej osobie, nawet po utracie ważności,
   g) musi być zabezpieczone przez Użytkownika przed nieuprawnionym dostępem osób trzecich;
2. W przypadku nieumyślnego ujawnienia hasła osobie nieuprawnionej lub podejrzenia ujawnienia, należy bezzwłocznie powiadomić ASI i dokonać zmiany hasła na nowe;
3. System informatyczny, w którym przetwarzane są dane osobowe automatycznie wymusza zmianę hasła **nie rzadziej niż co 90 dni**;
4. ASI może, w uzasadnionych sytuacjach, polecić dokonanie zmiany hasła przez Użytkownika oraz zapewniać automatyczną weryfikację spełniania wymogów dotyczących hasła;

## § 11.
## Wygaszacze ekranu.

1. Wygaszacze ekranu systemowo ustawiane są na aktywację po 10 minutach bezczynności na danej stacji roboczej oraz w razie potrzeby (np. opuszczenie miejsca przetwarzania danych) skrótem klawiaturowym;
2. Uruchomienie wygaszacza ekranu wiąże się z koniecznością ponownego zalogowania, celem wznowienia pracy stacji roboczej.

## Rozdział 3.
## Procedury rozpoczynania, zawieszania i kończenia pracy w systemie informatycznym.

### § 12.
### Rozpoczęcie pracy.

1. Procedura rozpoczęcia pracy w systemie informatycznym następuje poprzez zalogowanie się Użytkownika do komputera przez podanie loginu i hasła dostępu;
2. W przypadku nieodblokowania systemu, należy niezwłocznie zawiadomić ASI;
3. W przypadku zapomnienia przez Użytkownika konstrukcji hasła, winien on niezwłocznie zawiadomić ASI, który nadaje nowe hasło, postępując zgodnie z procedurą obowiązującą przy nadawaniu uprawnień dostępu do systemu informatycznego.

### § 13.
### Zawieszenie pracy.

1. Ustala się następującą procedurę zawieszenia pracy w systemie informatycznym:
   a) przy każdorazowym opuszczeniu stanowiska komputerowego, należy dopilnować, aby osoby postronne nie miały dostępu do danych przetwarzanych na tym stanowisku,
   b) każdy Użytkownik ma obowiązek stosowania wygaszacza ekranu zabezpieczonego hasłem oraz wylogowania się z systemu lub jego blokowania,
   c) zablokowanie komputera odbywa się poprzez naciśnięcie kombinacji klawiszy,
   d) niezależnie od powyższego, wygaszacz ekranu aktywuje się nie później niż w 10 minucie bezczynności Użytkownika,
   e) odblokowanie odbywa się poprzez ponowne zalogowanie się tego samego Użytkownika,
2. W pomieszczeniu, w którym przetwarzane są dane osobowe mogą znajdować się osoby postronne wyłącznie za zgodą i w towarzystwie Użytkownika lub innej upoważnionej osoby;
3. W przypadku zawieszenia pracy w systemie informatycznym z powodu konieczności załatwienia sprawy z osobą postronną znajdującą się w tym samym pomieszczeniu, Użytkownik ma obowiązek zabezpieczenia ekranu komputera lub urządzenia mobilnego oraz dokumentów i wydruków znajdujących się na biurku w sposób uniemożliwiający podgląd zawartych w nich treści.

### § 14.
### Zakończenie pracy.

1. Zakończenie pracy w systemie informatycznym polega na wybraniu odpowiedniego polecenia systemowego umożliwiającego zakończenie pracy;
2. Zaleca się zamknięcie wszystkich programów i zapisanie wszystkich otwartych plików. Użytkownik powinien pozostać przy komputerze do chwili ich zamknięcia;
3. Użytkownik kończący pracę powinien sprawdzić, czy wszystkie elektroniczne nośniki informacji lub wydruki i dokumenty zawierające dane osobowe zostały zabezpieczone przed dostępem osób nieupoważnionych;
4. Osoba opuszająca pomieszczenie jako ostatnia powinna zamknąć okna oraz zamknąć drzwi od pomieszczenia na klucz.

## Rozdział 4.
## Procedury użytkowania urządzeń mobilnych i elektronicznych nośników informacji. Korzystanie z Internetu. Poczta elektroniczna.

### § 15.

1. Przy przetwarzaniu danych osobowych na urządzeniach mobilnych oraz elektronicznych nośnikach informacji należy stosować procedury obowiązujące w przypadku użytkowania komputerów i urządzeń stacjonarnych;
2. Użytkownicy, którym zostały powierzone urządzenia mobilne oraz elektroniczne nośniki informacji, powinni chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych. Szczególną ostrożność należy zachować podczas ich transportu;
3. Obowiązuje zakaz używania urządzeń mobilnych oraz elektronicznych nośników informacji przez osoby inne niż Użytkownicy, którym zostały one powierzone;
4. Pliki zawierające dane osobowe przechowywane na urządzeniach mobilnych elektronicznych nośnikach informacji muszą być zaszyfrowane i opatrzone hasłem dostępu;
5. Urządzenia mobilne i elektroniczne nośniki informacji muszą być wyposażone w odpowiednie programy ochrony antywirusowej. Za tryb i sposób aktualizowania programów ochrony antywirusowej na urządzeniach mobilnych i elektronicznych nośników informacji odpowiada ASI.

### § 16.
### Korzystanie z Internetu.

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych;
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT i tylko w uzasadnionych przypadkach;
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu bez zgody i wiedzy ASI;
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo;
5. W opcjach przeglądarki internetowej zabrania się włączania opcji autouzupełniania formularzy i zapamiętywania haseł;
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:". Dla pewności należy „kliknąć" na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel;
7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet.

## § 17.
## Poczta elektroniczna.

1. Przesyłanie danych osobowych z użyciem poczty elektronicznej poza ZUK może odbywać się tylko przez osoby do tego upoważnione;
2. W przypadku przesyłania danych osobowych poza ZUK należy wykorzystywać mechanizmy kryptograficzne;
3. Hasło zabezpieczające wysyłane pliki powinno zawierać minimum 12 znaków: duże i małe litery i cyfry lub znaki specjalne. Hasło należy przesłać adresatowi odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em;
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu wysyłanego pocztą elektroniczną;
5. Zaleca się, aby Użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata;
6. Bez weryfikacji wiarygodności nadawcy zabrania się otwierania nieznanych załączników (plików) otrzymanych w e-mailach nawet od znanych nadawców;
7. Bez weryfikacji wiarygodności nadawcy, zabrania się „klikać" na hiperlink w otrzymanym e-mailu;
8. Każdy przypadek otrzymania e-maila o wątpliwej wiarygodności należy zgłaszać do ASI;
9. Zabrania się rozsyłania wiadomości prywatnych z wykorzystaniem konta służbowego;
10. Przy wysyłaniu korespondencji zbiorowej należy zawsze użyć opcji UDW – ukryte do wiadomości;
11. Konto w służbowej poczcie elektronicznej nie może być wykorzystywane do celów prywatnych;
12. Użytkownicy mają prawo korzystać ze służbowej poczty elektronicznej dla celów prywatnych wyłącznie okazjonalnie w sposób ograniczony do niezbędnego minimum;
13. Korzystanie z maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych;
14. Przy korzystaniu z poczty elektronicznej, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego;
15. Użytkownicy nie mogą korzystać ze służbowej poczty elektronicznej w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania (molestowanie, mobbing)
16. Użytkownik bez zgody Pracodawcy / Zleceniodawcy nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy / Zleceniodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej

## Rozdział 5.
## Zabezpieczanie danych w systemie informatycznym.

### § 18.
### Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

1. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
2. Za tworzenie i przechowywanie kopii zapasowych, o których mowa w ust. 1, w sposób zgodny z przepisami, o których mowa w § 1 oraz niniejszej Instrukcji odpowiedzialny jest ASI;
3. Dostęp do kopii zapasowych posiada wyłącznie ASI lub w wyjątkowych wypadkach, osoba upoważniona przez ADO.

### § 19.

### Sposób, miejsce i okres przechowywania kopii zapasowych i elektronicznych nośników informacji

1. Kopie zapasowe i elektroniczne nośniki informacji przechowywane są w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem, innych niż pomieszczenia serwerowni;
2. Kopie zapasowe i elektroniczne nośniki informacji przechowywane są przez okres, w którym istnieją przesłanki do ich przetwarzania. Po ustaniu przesłanek, o których mowa w zdaniu pierwszym, dane znajdujące się na kopiach zapasowych muszą zostać usunięte w sposób uniemożliwiający ich odtworzenie;
3. Kopie awaryjne należy bezzwłocznie usuwać po ustaniu ich użyteczności w przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych.

### § 20.
### Sposób zabezpieczania systemu informatycznego.

1. Zasady zachowania bezpieczeństwa w systemie informatycznym obejmują wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę informacji, stanowiących tajemnicę służbową przed ich nieuprawnionym przetwarzaniem oraz utratą danych spowodowaną awarią zasilania lub zakłóceniami sieci zasilającej;
2. System informatyczny musi być chroniony równolegle na wielu poziomach m.in. poprzez stosowanie oprogramowania antywirusowego, systemów typu firewall, odpowiednią konfigurację systemu aktualizacji systemu operacyjnego oraz realizację kopii bezpieczeństwa;
3. Oprogramowanie antywirusowe jest instalowane na wszystkich stanowiskach komputerowych oraz urządzeniach mobilnych i elektronicznych nośnikach informacji;
4. Aktualizacja oprogramowania antywirusowego odbywa się nie rzadziej niż raz w tygodniu, w sposób automatyczny dla wszystkich komputerów zainstalowanych w sieci;

5. Użytkownik na stanowisku komputerowym, importujący dane do systemu informatycznego jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości występowania wirusów i szkodliwego oprogramowania;
6. O pojawiających się komunikatach wskazujących na wystąpienie zagrożenia spowodowanego szkodliwym oprogramowaniem, użytkownik jest zobowiązany niezwłocznie powiadomić ASI;
7. Za wdrożenie, oraz aktualizację i korzystanie z oprogramowania, o którym mowa w ust. 2 odpowiada ASI.

**§ 21.**
**Monitorowanie systemu informatycznego.**

1. W celu zapewnienia ochrony systemu informatycznego stosuje się monitoring wykorzystania infrastruktury informatycznej, w szczególności obejmujący następujące elementy:
   a) analizę oprogramowania wykorzystanego na stacjach roboczych;
   b) analizę stacji roboczych pod względem wykorzystania nielegalnego oprogramowania, plików multimedialnych oraz innych elementów naruszających prawo autorskie;
   c) analizę odwiedzanych stron www;
   d) analizę godzin pracy na stanowiskach komputerowych;
   e) analizę dostępów (autoryzowanych oraz nieautoryzowanych);
   f) analizę ruchu sieciowego pod względem komunikacji, szkodliwej dla bezpieczeństwa danych przetwarzanych w systemie;
2. Monitoring bezpieczeństwa musi odbywać się z zachowaniem obowiązującego prawa

**§ 22.**
**Udostępnianie danych w systemie informatycznym.**

1. Dla każdej osoby, której dane są przetwarzane, system informatyczny służący do przetwarzania danych osobowych (z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie) zapewniają odnotowanie:
   a) daty pierwszego wprowadzenia danych do systemu,
   b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu,
   c) źródła danych (jedynie w przypadku zbierania danych nie od osoby, której dotyczą)
   d) informacji o odbiorcach;
   e) sprzeciwu odnośnie przetwarzania danych osobowych.
2. Dla każdej osoby, której dane osobowe są przetwarzane, system informatyczny zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1 pkt 1-5;
3. Odnotowanie informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia (z wyłączeniem osób, których dane dotyczą, osób posiadających upoważnienie do przetwarzania danych, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem), odbywa się poprzez zapisanie tej informacji w utworzonym na dysku twardym komputera pliku dotyczącym danej osoby

## § 23.
## Obowiązki ASI
## w zakresie zabezpieczenia systemu informatycznego

1. Do obowiązków ASI w zakresie zabezpieczenia systemu informatycznego należy :
   a) nadzór nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemów,
   b) nadzór nad czynnościami związanymi ze sprawdzaniem systemów pod kątem obecności wirusów komputerowych, częstości ich sprawdzania oraz wykonywania procedur uaktualniania systemów antywirusowych i ich konfiguracji,
   c) nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych oraz wszystkimi innymi czynnościami wykonywanymi na bazach danych osobowych,
   d) nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji,
   e) nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolą dostępu do danych osobowych, w tym zarządzanie kontami użytkowników (ustalenie identyfikatorów i haseł, ich przyznawanie, anulowanie, resetowanie i ochrona) oraz w porozumieniu z IOD dbałość o właściwe ustawienie urządzeń, tak aby minimalizować możliwość nieuprawnionego dostępu,
   f) podejmowanie natychmiastowych działań zabezpieczających stan systemów informatycznych w przypadku otrzymania informacji o naruszeniu zabezpieczeń, informacji o zmianach w sposobie działania systemu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych, w tym podjęcie działań mających na celu wykrycie przyczyny lub sprawcy zaistniałej sytuacji i jej usunięcie.

## § 24.

1. W celu zabezpieczenia integralności systemu informatycznego ASI może wykorzystywać w trakcie pracy oprogramowanie lub narzędzia monitorujące i rejestrujące aktywność Użytkowników na stanowiskach komputerowych;
2. Zabezpieczenie integralności systemu informatycznego realizowane jest również poprzez zakaz:
   a) wysyłania masowej poczty kierowanej do losowych odbiorców (spam),
   b) przechowywania w systemie informatycznym treści łamiących prawo autorskie (filmy, utwory muzyczne lub oprogramowanie),
   c) nieuzasadnionego wynoszenia lub wysyłania danych osobowych poza obszar przetwarzania danych,
   d) instalowania przez Użytkownika oprogramowania na sprzęcie komputerowym, które nie uzyskało akceptacji ASI
   e) wykorzystywania przeglądarek internetowych, które nie uzyskały akceptacji ASI oraz odwiedzania witryn internetowych zawierających potencjalnie niebezpieczne treści,
   f) podłączania innych urządzeń niż teleinformatyczne do wydzielonej instalacji elektrycznej (gniazdka w kolorze czerwonym),

g) przemieszczania sprzętu komputerowego do innej lokalizacji (pokoju) lub zmiany Użytkownika bez uzgodnienia z ASI;

h) fizycznego ingerowania w konfigurację sprzętową urządzeń,

i) podejmowania prób wykorzystania obcego konta, uruchamiania aplikacji deszyfrujących hasła, prowadzenia działań mających na celu podsłuchanie lub przechwycenie informacji przepływających w systemach informatycznych,

3. Dla zachowania integralności systemu informatycznego ASI może podjąć decyzję o:
   a) deinstalacji niebezpiecznego oprogramowania,
   b) usunięciu nielegalnych, niebezpiecznych oraz utrudniających wykonanie kopii bezpieczeństwa plików,
   c) zablokowaniu dostępu Użytkownika w przypadku stwierdzenia, że komputer lub urządzenie dołączone do generuje strumień danych zakłócający pracę sieci lub w razie podejrzenia używania komputera jako niezarejestrowanego serwera danych. O tym fakcie powiadamiany jest IOD i bezpośredni przełożony Użytkownika,
   d) w porozumieniu z IOD, zablokowaniu konta Użytkownika.

## §25.
## Procedury wykonywania przeglądów i konserwacji systemu informatycznego.

1. Dla zachowania ciągłości pracy i bezpieczeństwa danych przeprowadza się przegląd i konserwację platformy sprzętowej, na której eksploatowany jest system informatyczny wykorzystywany w Ośrodku;
2. Przeglądy i konserwacja urządzeń wchodzących w skład platformy sprzętowej, o której mowa w ust. 1 powinny być wykonywane nie rzadziej niż w terminach określonych przez producenta sprzętu;
3. Jeśli producent nie przewidział dla danego urządzenia potrzeby dokonywania przeglądów eksploatacyjnych lub nie określił ich częstotliwości, to o dokonaniu przeglądu oraz sposobie jego przeprowadzenia decyduje ASI;
4. Wszelkie naprawy urządzeń komputerowych, w tym urządzeń mobilnych i elektronicznych nośników informacji, oraz zmiany w systemie informatycznym przeprowadza, w miarę możliwości, ASI;
5. Jeżeli do przywrócenia prawidłowego działania systemu niezbędna jest pomoc podmiotu zewnętrznego, wszelkie czynności na sprzęcie komputerowym dokonywane w obszarze przetwarzania danych osobowych, powinny odbywać się w obecności ASI;
6. W przypadku niemożności dokonania naprawy uszkodzonego sprzętu komputerowego zawierającego dane osobowe, należy go zniszczyć mechanicznie w sposób trwale uniemożliwiający odczytanie jego zawartości;
7. Konserwację oprogramowania przeprowadza się po zgłoszeniu przez Użytkownika potrzeby wprowadzenia zmian pozwalających dostosować ich funkcjonalność do obsługi bieżących lub planowanych potrzeb. Zgłoszenia rozpatruje ASI;

**§ 26.**

1. Nieprawidłowości ujawnione w trakcie przeglądów bądź konserwacji, powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane przez ASI;
2. Przegląd aplikacji przeprowadzany jest w celu sprawdzenia poprawności działania i wykonywany jest w następujących przypadkach:
   a) zmiany wersji oprogramowania aplikacji,
   b) zmiany systemu operacyjnego platformy sprzętowej, na której eksploatowana jest aplikacja,
   c) wykonania zmian w aplikacji spowodowanych koniecznością naprawy lub modyfikacji systemu;
3. Przed dokonaniem zmian w aplikacji należy, o ile to możliwe, dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych, na testowej bazie danych. Sprawdzenie powinno obejmować w szczególności:
   a) poprawność logowania się do systemu w zależności od posiadanych uprawnień (symulacja pracy wszystkich typów uprawnień Użytkownika),
   b) techniczną poprawność działania aplikacji.

**§ 27.**

**Procedura w przypadku stwierdzenia naruszenia zasad bezpieczeństwa systemu informatycznego.**

1. W przypadku stwierdzenia przez Użytkownika naruszenia zabezpieczeń systemu informatycznego przez osoby nieuprawnione, jest on zobowiązany niezwłocznie poinformować o tym fakcie ASI oraz IOD;
2. ASI jest zobowiązany niezwłocznie podjąć czynności zmierzające do ustalenia przyczyn naruszeń zasad bezpieczeństwa i zastosować środki uniemożliwiające ich naruszanie w przyszłości;
3. W przypadku wykrycia zagrożenia automatycznym działaniem, możliwe jest zablokowanie pracy w systemie do chwili podjęcia decyzji o sposobie postępowania;
4. W celu minimalizacji zagrożeń dąży się, w miarę możliwości organizacyjnych, do maksymalnej unifikacji sprzętu, stosowanego oprogramowania, konfiguracji sprzętu i oprogramowania, a także rozwiązań organizacyjnych.

## Rozdział 6.
## Realizacja minimalnych wymagań dla systemów teleinformatycznych wymaganych Krajowymi Ramami Operacyjności (KRI)

### § 28.

1. Zakład Usług Komunalnych w Węglińcu, ul. Partyzantów 8, 59-940 Węgliniec, realizujący zadania publiczne, opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność integralność i rozliczalność informacji.
2. Zarządzanie bezpieczeństwem informacji realizowane jest poprzez:
   a) aktualizację regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia
   b) utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację
   c) przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy ryzyka
   d) podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji
   e) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób zaangażowanych w procesy przetwarzania informacji
   f) szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak zagrożenia bezpieczeństwa informacji i skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna
   g) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich
   h) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
      - dbałości o aktualizację oprogramowania,
      - minimalizowaniu ryzyka utraty informacji w wyniku awarii,
      - ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
      - stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
      - zapewnieniu bezpieczeństwa plików systemowych,
      - redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
   i) niezwłoczne podejmowanie działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa
   j) kontrole zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa
   k) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony z góry i ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;
   l) realizowane okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji - nie rzadziej niż raz na rok.

**§ 29.**

1. Rozliczalność w systemach teleinformatycznych wykorzystywanych w ZUK podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach).

2. W dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do:
   - systemu z uprawnieniami administracyjnymi;
   - konfiguracji systemu, w tym konfiguracji zabezpieczeń;
   - przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa

**§ 30.**

1. W ZUK używane systemy teleinformatyczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.

2 Zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury.

**§ 31.**

1. Poza informacjami wymienionymi w § 29.mogą być odnotowywane działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci:
   - działań użytkowników nieposiadających uprawnień administracyjnych,
   - zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu,
   - zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny – w zakresie wynikającym z analizy ryzyka.

Informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.

## Rozdział 6.
## Postanowienia końcowe.

**§ 32.**

3. W sprawach nieuregulowanych niniejszą Instrukcją, znajdują zastosowanie przepisy wymienione w § 1;
4. Nad aktualnością Instrukcji czuwa IOD w porozumieniu z ASI;
5. IOD we współpracy z ASI może prowadzić kontrolę przestrzegania Instrukcji. Wyniki kontroli doraźnych przedstawiane są ADO.

Załącznik Nr 3
do Zarządzenia
Dyrektora
Nr 02/2022
z dnia 12.10.2022

....., dnia .....

Nazwisko i imię pracownika .....

Stanowisko .....

## OŚWIADCZENIE

Pouczona/y o odpowiedzialności oświadczam, że zapoznałam/em się z postanowieniami Polityki Bezpieczeństwa Informacji oraz Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych w Zakładzie Usług Komunalnych w Węglińcu, ul. Partyzantów, 59-940 Węgliniec reprezentowany przez Dyrektora i zobowiązuję się do przestrzegania wynikających z nich zasad.

.....

podpis osoby składającej oświadczenie