

Załącznik Nr 1
do Zarządzenia nr 13/2018
Wójta Gminy Olszówka
z dnia 25.09.2018 r.

POLITYKA OCHRONY DANYCH

ZATWIERDZAM

WÓJT

25.09 '18r.

Włodzimierz Fraszczyk

(data i podpis Administratora Danych)

Spis treści

I. POSTANOWIENIA OGÓLNE	3
DEKLARACJA I ZASTOSOWANIE	3
DEFINICJE	4
ZASADY OCHRONY DANYCH.....	6
ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO DANYCH OSOBOWYCH	7
II. OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH	8
III. PRZEDSIĘWZIĘCIA ZABEZPIECZAJĄCE PRZED NARUSZENIEM OCHRONY DANYCH.....	9
IV. POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH.....	11
DZIAŁANIA KORYGUJĄCE I ZAPOBIEGAWCZE.....	11
ZGŁASZANIE NARUSZEŃ.....	11
V. DOSTĘP DO DANYCH OSOBOWYCH	11
VI. PRAWA I ŻĄDANIA PODMIOTÓW DANYCH.....	12
POROZUMIENIA I KONTAKTY ZE STRONAMI ZEWNĘTRZNYMI.....	12
VII. GRUPY INFORMACJI PODLEGAJĄCE OCHRONIE I REJESTR CZYNNOŚCI	13
VIII. BEZPIECZEŃSTWO OSOBOWE.....	13
ETAP NABORU PRACOWNIKA I WSPÓŁPRACOWNIKA.....	14
EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH.....	14
ZATRUDNIENIE / WSPÓŁPRACA	15
ZAKOŃCZENIE ZATRUDNIENIA / WSPÓŁPRACY.....	15
ZASADY PRZYZNAWANIA DOSTĘPU	16
IX. BEZPIECZEŃSTWO TELEINFORMATYCZNE	16
AUTORYZACJA I DOPUSZCZALNE WYKORZYSTANIE ZASOBÓW.....	16
METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM.....	18
X. POSTANOWIENIA KOŃCOWE	19
XI. SPIS ZAŁĄCZNIKÓW	21

I. POSTANOWIENIA OGÓLNE

§ 1

DEKLARACJA I ZASTOSOWANIE

1. **Celem** niniejszej Polityki bezpieczeństwa danych osobowych (**PODO**) jest wypełnienie założeń Rozporządzenia 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, dalej też zwane **RODO**).
2. Stanowi ona zbiór wymogów, zasad i regulacji ochrony danych osobowych u **Administradora danych osobowych**, którym jest **Gmina Olszówka** z siedzibą w **Olszówka, Olszówka 15; 62-641 Olszówka**, reprezentowana przez **Wójta Gminy Olszówki**, (dalej jako **ADO**).
3. Zasady, działania, kompetencje i zakresy odpowiedzialności opisane w niniejszej Polityce Ochrony Danych Osobowych (**PODO** lub **Polityka**), obowiązują wszystkich pracowników i współpracowników **ADO**.
4. Procedury i dokumenty związane z **Polityką** będą weryfikowane i dostosowywane w celu zapewnienia odpowiedniego poziomu bezpieczeństwa. Przeglądy dokumentacji odbywają się nie rzadziej niż raz w roku. Wzór *Plan audytu i przeglądów Polityki ochrony danych osobowych* stanowi **załącznik nr 7** do niniejszej Polityki.
5. Polityka określa środki techniczne i organizacyjne zastosowane przez **ADO** dla zapewnienia ochrony danych oraz tryb postępowania w przypadku stwierdzenia naruszenia zabezpieczenia danych w systemie informatycznym lub w kartotekach papierowych, albo w sytuacji podejrzenia o takim naruszeniu.
6. Polityka została opracowana z uwzględnieniem metod i środków ochrony danych, których skuteczność w czasie ich zastosowania jest powszechnie uznawana. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania właściwej ochrony wraz z zachowaniem ich integralności i rozliczalności, ze szczególnym uwzględnieniem obowiązujących przepisów prawa dotyczących ochrony danych osobowych.
7. Zakres obowiązywania dokumentu.
 - 1) Niniejsza **Polityka** obowiązuje wszystkich pracowników, współpracowników, a także kontrahentów **ADO**.
 - 2) Każdy z pracowników i współpracowników ma obowiązek zapoznania się z treścią niniejszej **Polityki**.
 - 3) Polityka dotyczy wyposażenia, systemów, urządzeń przetwarzających informacje w formie elektronicznej, papierowej lub jakiegokolwiek innej.

- 4) Nieprzestrzeganie postanowień zawartych w **Polityce** może skutkować sankcjami w pełnym zakresie dopuszczonym przez stosunek pracy oraz obowiązujące przepisy prawa.
- 5) W celu skutecznego zapoznania pracowników i współpracowników z zasadami zawartymi w niniejszej Polityce wprowadza się zestaw reguł stanowiący wyciąg najistotniejszych zapisów zawartych w **Polityce**. *Zasady użytkowania zasobów komputerowych i sieci komunikacyjnych* opisane są w **załączniku nr 12** do niniejszej **Polityki**.

Odpowiedzialny za wdrożenie i utrzymanie niniejszej **Polityki** jest ADO, a za nadzór i monitorowanie jej przestrzegania odpowiada: ***Inspektor ochrony danych (dalej IOD)***.

§ 2

DEFINICJE

Administrator - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. **Administratorem danych osobowych jest Gmina Olszówka, reprezentowana przez Dyrektora (dalej jako ADO).**

Administrator Systemu Informatycznego (ASI) - rozumie się przez to osobę odpowiedzialną za nadzór nad systemami informatycznymi wykorzystywanymi u Administratora Danych. Wyznaczenie i obowiązki ASI opisuje **załącznik nr 2** do niniejszej **Polityki**.

bezpieczeństwo informacji - zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;

dane osobowe - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

hasło - rozumie się przez to ciąg znaków alfanumerycznych, znany jedynie użytkownikowi;

identyfikator - rozumie się przez to, ciąg znaków literowych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

incydent ochrony danych osobowych - zdarzenie albo seria niepożądanych lub niespodziewanych zdarzeń ochrony danych osobowych stwarzających znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrożenia ochrony danych osobowych;

Inspektor ochrony danych (IOD) - osoba sprawująca nadzór nad przestrzeganiem zasad ochrony danych osobowych wyznaczona przez **ADO**; *wyznaczenie i zakres obowiązków IOD* opisuje **załącznik nr 1**, a *regulamin IOD* **załącznik nr 14** do niniejszej **Polityki**.

naruszenie ochrony danych osobowych - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania,

nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

obszar przetwarzania danych - rozumie się przez to budynki i pomieszczenia określone przez administratora danych, tworzące obszar, w którym przetwarzane są dane osobowe i inne informacje prawem chronione; obszar przetwarzania danych opisany jest w **załączniku nr 3** do niniejszej **Polityki**;

odbiorca danych - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią; organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

osoba, podmiot danych - oznacza osobę, której dane dotyczą;

podmiot przetwarzający - oznacza organizację lub osobę, której ADO powierzył przetwarzanie danych osobowych (np. usługodawca IT, dostawca ESOK czy innego systemu informatycznego);

polityka oznacza niniejszą politykę ochrony danych osobowych;

postępowanie z ryzykiem - proces planowania i wdrażania działań wpływających na ryzyko;

poufność danych - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

raport - rozumie się przez to przygotowanie przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;

RCPDO lub rejestr oznacza rejestr czynności przetwarzania danych osobowych;

RODO oznacza rozporządzenie parlamentu europejskiego i rady (UE) 2016/679 z 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) (dz. urz. UE L 119, s. 1).

ryzyko - niepewność osiągnięcia zamierzonych celów;

serwisant - rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego;

system informatyczny administratora danych - rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych;

szacowanie ryzyka - proces identyfikowania, analizowania i oceniania ryzyka;

Teczka ODO - zbiór dokumentów, instrukcji, regulaminów, załączników opisujących sposób przetwarzania i ochrony danych, składający się na politykę ochrony danych osobowych, gromadzonych i nadzorowanych przez IOD.

teletransmisja - rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;

uwierzytelnienie - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

użytkownik - rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło;

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

§ 3

ZASADY OCHRONY DANYCH

System zarządzania ochroną danych osobowych zgodny z wymaganiami niniejszej Polityki działa z poszanowaniem następujących zasad:

- 1) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
- 2) rzetelnie i uczciwie (rzetelność);
- 3) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
- 4) w konkretnych celach i nie "na zapas" (minimalizacja);
- 5) nie więcej niż potrzeba (adekwatność);
- 6) z dbałością o prawidłowość danych (prawidłowość);
- 7) nie dłużej niż potrzeba (czasowość);
- 8) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

§ 4

1. W celu zwiększenia efektywności ochrony danych osobowych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Jest ona realizowana poprzez: zabezpieczenia fizyczne, zabezpieczenia logiczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu poniższych celów i zapewnić:
 - 1) **rozliczalność** - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
 - 2) **integralność** - rozumie się przez to właściwość zapewniającą, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
 - 3) **poufność** - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
 - 4) **integralność systemu** - rozumianą jako nienaruszalność systemu, niemożność jakiegokolwiek manipulacji, zarówno zamierzonej jak i przypadkowej.
 - 5) **dostępność** - gwarantuje, że osoby, które są upoważnione i którym informacje są potrzebne, mają do nich dostęp w odpowiednim miejscu i czasie.
 - 6) **uwierzytelnienie** - uwiarygodnienie swojej tożsamości względem systemu teleinformatycznego;
 - 7) **autentyczność** - właściwość zapewniająca, że tożsamość podmiotu lub procesu jest taka, jak deklarowana;
3. Cele i strategie bezpieczeństwa:
 - 1) zgodność z prawem,
 - 2) ochrona zasobów informacyjnych i innych aktywów,

- 3) uzyskanie i utrzymanie odpowiednio wysokiego poziomu bezpieczeństwa zasobów, rozumiane jako zapewnienie poufności, integralności i dostępności zasobów oraz zapewnienie rozliczalności podejmowanych działań,
- 4) zapewnienie ciągłości działania procesów i właściwej reakcji na incydenty,
- 5) zapewnienie odpowiedniego poziomu wiedzy dotyczącej ochrony danych osobowych wśród pracowników i współpracowników poprzez zapewnienie odpowiednich szkoleń.

§ 5

ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO DANYCH OSOBOWYCH

1. **ADO** zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez **ADO**.
2. **ADO** przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. *Procedura zarządzania ryzykiem* stanowi **załącznik nr 8** do niniejszej **Polityki**.
3. Za bezpieczeństwo danych osobowych u **ADO** odpowiedzialni są wszyscy pracownicy. W szczególności odpowiadają oni za przestrzeganie zasad bezpieczeństwa wynikających z niniejszej Polityki oraz zgłaszanie incydentów i naruszeń, a także wykonywanie zaleceń **IOD**.
4. We wszystkich umowach, które mogą dotyczyć przetwarzania danych u **ADO**, należy uwzględnić zapisy zobowiązujące drugą stronę do przestrzegania art. 28 **RODO** oraz obowiązujących przepisów krajowych.
5. Inspektor ochrony danych prowadzi rejestr podmiotów zewnętrznych, z którymi realizacja umów/porozumień/zamówień lub aneksów do nich zobowiązuje lub umożliwia zleceniobiorcy/wykonawcy dostęp do informacji zawierających dane osobowe.
6. Za przestrzeganie zasad ochrony danych osobowych i za codzienną ochronę danych odpowiedzialni są upoważnieni użytkownicy.

§ 6

Realizację zamierzeń określonych w § 3 powinny zagwarantować następujące założenia:

- 1) Wdrożenie procedur określających postępowanie osób dopuszczonych do przetwarzania informacji oraz ich odpowiedzialność za ochronę danych.
- 2) Przeszkolenie użytkowników w zakresie ochrony danych osobowych.
- 3) Przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory).
- 4) Podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń.
- 5) Okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych.
- 6) Opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii.
- 7) Okresowe aktualizowanie **Polityki**.
- 8) Identyfikacja zagrożeń i analiza ryzyka.

II. OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH

§ 7

Podział zagrożeń:

- 1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
- 2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
- 3) zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

§ 8

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są informacje to głównie:

- 1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
- 2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy,
- 3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
- 4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
- 5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
- 6) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych,
- 7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
- 8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
- 9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,

- 10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony informacji - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
- 11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.,
- 12) podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane,
- 13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur ochrony danych osobowych (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych, itp.).

§ 9

Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.

Procedura zgłaszania naruszeń stanowi załącznik nr 9 do niniejszej Polityki.

III. PRZEDSIĘWZIĘCIA ZABEZPIEZAJĄCE PRZED NARUSZENIEM OCHRONY DANYCH

§ 10

1. Każdy użytkownik - przed dopuszczeniem do przetwarzania danych osobowych podlega przeszkoleniu z przepisów w tym zakresie oraz wynikających z nich zadań i obowiązków.
2. Wszyscy użytkownicy podlegają okresowym szkoleniom.
3. Za organizację szkoleń odpowiedzialny jest Inspektor ochrony danych.

§ 11

1. Dla zapewnienia bezpieczeństwa danych zastosowano następujące **środki organizacyjne**:
 - 1) Dostęp do danych osobowych mogą mieć tylko i wyłącznie użytkownicy posiadający pisemne, imienne upoważnienia nadane przez Administratora Danych.
 - 2) Każdy z pracowników powinien zachować szczególną ostrożność przy przenoszeniu wszelkich nośników z danymi.
 - 3) Należy chronić dane przed wszelkim dostępem do nich osób nieuprawnionych.
 - 4) Pomieszczenia w których są przetwarzane dane osobowe muszą być zamykane na klucz.

- 5) Dostęp do kluczy posiadają tylko upoważnieni pracownicy.
 - 6) Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy. W wypadku gdy jest wymagany poza godzinami pracy - możliwy jest tylko na podstawie zezwolenia Administratora Danych lub **IOD**.
 - 7) Dostęp do pomieszczeń w których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy.
 - 8) W przypadku pomieszczeń do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganych na wykonanie niezbędnych czynności.
 - 9) Szafy w których przechowywane są dane powinny być zamykane na klucz.
 - 10) Klucze do tych szaf posiadają tylko upoważnieni pracownicy.
 - 11) Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych a następnie powinny być zamykane.
 - 12) Dane w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych a następnie muszą być chowane do szaf.
2. Dla zapewnienia bezpieczeństwa danych i informacji zastosowano następujące **środki techniczne**:
- 1) Dostęp do komputerów na których są przetwarzane dane mają tylko upoważnieni pracownicy.
 - 2) Monitory komputerów na których przetwarzane są dane są tak ustawione aby osoby nieupoważnione nie miały wglądu w dane.
 - 3) Po zakończeniu pracy komputery przenośne (np. typu notebook) zawierające dane osobowe powinny być zabezpieczone w zamykanych na klucz szafach.
 - 4) W wypadku potrzeby wyniesienia komputera przenośnego (np. typu notebook) zawierającego dane osobowe, lub inne informacje chronione, komputer taki musi być odpowiednio dodatkowo zabezpieczony, a dane zaszyfrowane.
 - 5) Nie należy udostępniać osobom nieupoważnionym tych komputerów.
 - 6) W przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności.
 - 7) Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie) aby nie zostały na nich dane osobowe.
 - 8) W wypadku niemożliwości skasowania danych z nośnika (płyta CD-ROM) należy taką płytę zniszczyć fizycznie.
 - 9) W przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków.
 - 10) Niezabezpieczonych danych osobowych nie należy przysyłać drogą elektroniczną.
 - 11) Sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz.
 - 12) Błędne lub nieaktualne wydruki i wersje papierowe zawierające dane osobowe lub inne informacje chronione niszczone są za pomocą niszczarki lub w inny mechaniczny sposób uniemożliwiający powtórne ich odtworzenie.

IV. POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH

§ 12

DZIAŁANIA KORYGUJĄCE I ZAPOBIEGAWCZE

1. Działania korygujące podejmowane są w przypadku wykrycia niezgodności w działalności, bądź nieprawidłowego działania procesu.
Przesłanką do podjęcia działań korygujących mogą być wyniki kontroli, audytów, zgłoszenia niezgodności, zdarzenia i incydenty związane z ochroną danych osobowych, zapisy, wyniki badania zadowolenia klientów, analiza reklamacji klientów.
Działania zapobiegawcze mają na celu zapobiec wystąpieniu potencjalnych niezgodności.

§ 13

ZGŁASZANIE NARUSZEŃ

ADO stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia - *Procedura zgłaszania naruszeń* stanowi **załącznik nr 9** do niniejszej **Polityki**.

V. DOSTĘP DO DANYCH OSOBOWYCH

§ 14

1. Przetwarzanie, w tym udostępnianie danych osobowych jest prawnie dopuszczalne, jeżeli jest niezbędne dla zrealizowania obowiązku wynikającego z przepisu prawa.
2. W przypadku udostępnienia danych osobowych w celach innych niż włączenie do rejestru, administrator danych udostępnia posiadane informacje osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
3. Dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
4. Podmiot występujący o udostępnienie informacji powinien wskazać podstawę prawną upoważniającą go do otrzymania tych danych albo uzasadnioną potrzebę żądania ich udostępnienia. Tylko w takiej sytuacji można dokonać oceny, czy w określonym przypadku udostępnienie danych jest prawnie dopuszczalne i czy nie będzie ono stanowiło naruszenia zasad ochrony informacji.
5. Przetwarzanie, w tym udostępnianie danych osobowych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą, oraz następuje w celu badań naukowych, dydaktycznych, historycznych oraz statystycznych.

6. Udostępnienie danych może nastąpić jedynie za zgodą Administratora danych lub **IOD** i powinno być odpowiednio udokumentowane.

§ 15

VI. PRAWA I ŻĄDANIA PODMIOTÓW DANYCH

Każdej osobie, której dane osobowe są przetwarzane przysługuje prawo do kontroli przetwarzania jej danych osobowych, a w szczególności prawo do:

- 1) uzyskania wyczerpującej informacji, czy jej dane osobowe są przetwarzane oraz do otrzymania informacji o pełnej nazwie i adresie siedziby Administratora Danych;
- 2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych osobowych;
- 3) uzyskania informacji, od kiedy są przetwarzane jej dane osobowe, oraz podania w powszechnie zrozumiałej formie treści tych danych;
- 4) uzyskania informacji o źródle, z którego pochodzą dane osobowe jej dotyczące;
- 5) uzyskania informacji o sposobie udostępniania danych osobowych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym te dane osobowe są udostępniane;
- 6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem przepisów prawa albo są już zbędne do realizacji celu, dla którego zostały zebrane.
- 7) *Polityka realizacji praw osób, których dane dotyczą*, sposoby informowania i komunikacji oraz tryb wykonywania praw przez osobę, której dane dotyczą opisane są w **załączniku nr 10** do niniejszej **Polityki**.

§ 16

POROZUMIENIA I KONTAKTY ZE STRONAMI ZEWNĘTRZNYMI.

1. Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą.
2. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, wiążąc podmiot przetwarzający i administratora, określając przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.
3. W przypadku zawierania umów z firmami zewnętrznymi mającymi wpływ na funkcjonowanie kluczowych elementów systemu zarządzania bezpieczeństwem informacji zalecane jest zawarcie umowy powierzenia.

ADO przyjął wymagania co do umowy powierzenia przetwarzania danych zawarte w *Polityce korzystania z usług podmiotów przetwarzających*, stanowiącej **załącznik nr 11** do niniejszej **Polityki**.

VII. GRUPY INFORMACJI PODLEGAJĄCE OCHRONIE I REJESTR CZYNNOŚCI

§ 17

1. Grupa informacji dotycząca działalności:
 - 1) dane osobowe patentów 2) dane osobowe wnioskodawców 3) dane osobowe pracowników i współpracowników
2. Grupa informacji dotycząca pracowników:
 - 1) prywatne dane osobowe pracowników,
 - 2) dane osobowe rodzin pracowników,
 - 3) dane osoby - kandydata do zatrudniania,
 - 4) informacje dot. obsługi kadrowo-płacowej pracownika (wynagrodzenia, ewidencja czasu pracy, informacja o urlopach) .
3. Grupa informacji dotycząca infrastruktury fizycznej i teleinformatycznej:
 - 1) dane o zabezpieczeniach systemu informatycznego,
 - 2) dane o zabezpieczeniach infrastruktury fizycznej,
 - 3) informacje dotyczące systemów zarządzania
 - 4) dokumentacja techniczna infrastruktury.
4. **Rejestr czynności przetwarzania danych osobowych (RCPDO)** stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli **zasady rozliczalności**.
5. W Rejestrze, dla każdej czynności przetwarzania danych, którą **ADO** uznał za odrębną odnotowuje co najmniej: (1) nazwę czynności, (2) cel przetwarzania, (3) opis kategorii osób i opis kategorii danych, (5) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu **ADO**, jeśli podstawą jest uzasadniony interes, (6) *Ż*, (7) opis kategorii odbiorców danych (w tym przetwarzających), (8) informację o przekazaniu poza **EU/EOG**; (9) ogólny opis technicznych i organizacyjnych środków ochrony danych.
6. Inspektor ochrony danych monitoruje prowadzenie Rejestru czynności przetwarzania danych osobowych. Wzór *Rejestru czynności przetwarzania* stanowi **załącznik nr 4** do niniejszej **Polityki**.

VIII. BEZPIECZEŃSTWO OSOBOWE

§ 18

ETAP NABORU PRACOWNIKA I WSPÓŁPRACOWNIKA

1. Do przetwarzania danych osobowych i do dostępu do innych informacji chronionych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych. Administrator danych może wydać pełnomocnictwo do nadawania upoważnień.
2. Wzór *upoważnienia do przetwarzania danych osobowych* stanowi **załącznik nr 6** do niniejszej Polityki. Upoważnienia rejestruje się w *ewidencji upoważnień*, stanowiącej **załącznik nr 13** do niniejszej **Polityki**.
3. Zakres upoważnienia może również być określony w umowie o pracę lub współpracę.
4. Osoba upoważniona zobowiązana jest podpisać oświadczenie lub umowę, która określa odpowiedzialność w zakresie ochrony danych osobowych.
5. Osoby upoważnione do przeprowadzania działań związanych z naborem powinny zwrócić szczególną uwagę na zasady ochrony danych wymienione w § 3 niniejszej Polityki, a także aktualnie obowiązujące przepisy prawa w tym zakresie.

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH

1. Prowadzenie Ewidencji osób upoważnionych do przetwarzania danych osobowych nadzoruje Inspektor ochrony danych. Wzór ewidencji stanowi **załącznik nr 13** do niniejszej **Polityki**.
2. Ewidencja zawiera:
 - 1) imię i nazwisko użytkownika,
 - 2) datę nadania i ustania upoważnienia
 - 3) zakres upoważnienia
 - 4) identyfikator użytkownika
3. Ewidencja użytkowników może być prowadzona w systemie informatycznym.
4. Zmiany dotyczące użytkownika, takie jak:
 - 1) zmiana imienia lub nazwiska,
 - 2) zmiana zakresu upoważnienia,podlegają niezwłocznemu odnotowaniu w ewidencji.
5. Zmiany dotyczące użytkownika, takie jak:
 - 1) rozwiązanie umowy,
 - 2) utrata upoważnienia do przetwarzania danych osobowych
 - 3) zmiana zakresu obowiązków służbowych skutkująca ustaniem upoważnienia,powodują wyrejestrowanie użytkownika przez Administratora Aplikacji oraz **ASI** w trybie natychmiastowym z ewidencji, zablokowanie identyfikatora oraz unieważnienie hasła tego użytkownika.
6. Osoba odpowiedzialna za sprawy kadrowe, bezpośredni przełożony Użytkownika, odpowiadają za natychmiastowe zgłoszenie do **ASI** użytkowników, którzy utracili uprawnienia do dostępu do danych osobowych, celem zablokowania im dostępu do systemu informatycznego poprzez zablokowanie identyfikatora i wyrejestrowanie z ewidencji osób upoważnionych.

7. Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi.

§ 19

ZATRUDNIENIE / WSPÓŁPRACA

1. Pracownicy, współpracownicy, wykonawcy i podwykonawcy powinni być świadomi swoich obowiązków i odpowiedzialności prawnej oraz zagrożeń związanych z bezpieczeństwem informacji. W tym celu należy zapewnić wszystkim zatrudnionym właściwy poziom świadomości poprzez kształcenie i szkolenie z zakresu ochrony danych osobowych, ze szczególnym uwzględnieniem procedur bezpieczeństwa. Dokumentują to:
 - lista obecności ze szkoleń,
 - oświadczenia pracowników,
 - umowy o poufności
 - posiadane zaświadczenia, dyplomy lub certyfikaty.
2. W przypadku naruszenia zasad ochrony danych osobowych jest uruchamiana odpowiednia procedura postępowania dyscyplinarnego, która powinna być poprzedzona potwierdzeniem naruszenia zasad ochrony danych osobowych i zgromadzeniem materiału dowodowego.
3. Postępowanie dyscyplinarne powinno uwzględniać: rodzaj i wagę naruszenia zasad ochrony danych osobowych, wpływ na procesy biznesowe, przypadek incydentalny czy jest to kolejne naruszenie oraz jakość odbytego przeszkolenia.
4. W przypadku pracy mobilnej i na odległość z wykorzystaniem urządzeń przenośnych zastosowano odpowiednie, dodatkowe środki bezpieczeństwa.
5. Przekazywanie sprzętu i urządzeń służących do przetwarzania danych odbywa się na podstawie protokołów przekazania sprzętu.

§ 20

ZAKOŃCZENIE ZATRUDNIENIA / WSPÓŁPRACY

1. Zakończenie zatrudnienia lub zmiana stanowiska pracy wewnątrz organizacji powinny odbywać się w sposób zorganizowany.
2. Odchodzenie z organizacji lub zmiana stanowiska pracy wiąże się ze zwrotem posiadanego przez pracownika sprzętu i odebraniem lub zmianą praw dostępu.
3. Odebranie lub ograniczenie praw dostępu jest poprzedzone analizą ryzyka uwzględniającą następujące uwarunkowania:
 - 1) ustalenie inicjatora (pracownik, wykonawca czy kierownictwo **ADO**) i przyczyn zakończenia lub zmiany zatrudnienia;
 - 2) aktualny zakres czynności pracownika, wykonawcy lub podwykonawcy;
 - 3) wartość aktualnie dostępnych aktywów.

§ 21

ZASADY PRYZNAWANIA DOSTĘPU

1. Przyznawanie zakresu uprawnień powinno być w ścisłym związku z zakresem obowiązków danego pracownika.
2. Zarządzanie dostępem na etapie nadawania, zmiany i cofania praw dostępu pracowników w obszarze przetwarzania danych oraz do systemów teleinformatycznych powinno się odbywać na wniosek bezpośredniego przełożonego Użytkownika.
3. W zarządzaniu dostępem obowiązuje zasada, że dostęp użytkownika powinien opierać się na spełnieniu zasady rozliczalności oraz zasady niezaprzeczalności. W przypadku systemów informatycznych obowiązują następujące wymagania:
 - 1) wymóg jednoznacznej identyfikacji pracownika - tj. w systemach informatycznych każdy użytkownik pracuje wyłącznie na swoim indywidualnym koncie, nie są stosowane konta anonimowe lub współdzielone poza wyjątkami, gdzie z przyczyn technicznych nie ma innej możliwości,
 - 2) wymóg uwierzytelnienia pracownika przy korzystaniu z systemu informatycznego,
 - 3) autoryzacji przyznania praw dostępu do systemów informatycznych.
 - 4) zasady przywilejów, wiedzy i usług koniecznych.

IX. BEZPIECZEŃSTWO TELEINFORMATYCZNE

§ 22

AUTORYZACJA I DOPUSZCZALNE WYKORZYSTANIE ZASOBÓW.

1. Przy ochronie zasobów kluczowe jest stosowanie podstawowej zasady bezpieczeństwa, że nie jest dozwolone wykorzystywanie zasobów w sposób inny niż jawnie dozwolony.
2. Do wykonywania obowiązków służbowych związanych z przetwarzaniem informacji dozwolone jest używanie systemów, urządzeń i oprogramowania dopuszczonych do użytku zgodnie z wymogami **Polityki**
3. Pracownicy są uprawnieni do korzystania z zasobów teleinformatycznych niezbędnych do wykonywania ich obowiązków. Szczegółowa *procedura przyznawania dostępu* stanowi **załącznik nr 15** do niniejszej Polityki.
4. Zakazane jest użytkowanie na terenie obszaru przetwarzania danych lub przy wykonywaniu obowiązków służbowych poza obszarem przetwarzania danych innych niż dopuszczone urządzeń, systemów i oprogramowania bez zgody Administratora Systemu Informatycznego (**ASI**).
5. Zakazane jest bez zgody **ASI**:
 - a) użytkowanie urządzeń skutkujących połączeniem systemów Administratora danych z sieciami teleinformatycznymi innych podmiotów, w tym publicznymi sieciami teleinformatycznymi,
 - b) użytkowanie urządzeń lub oprogramowania mających na celu zakłócenie działania innych systemów, urządzeń lub oprogramowania,

- c) użytkowanie urządzeń lub oprogramowania do testowania bezpieczeństwa lub wykrywania podatności,
 - d) użytkowanie urządzeń lub oprogramowania mogących naruszyć bezpieczeństwo innych systemów lub urządzeń,
 - e) wprowadzanie zmian konfiguracji urządzeń, systemów lub oprogramowania.
6. Zakazane jest bez zgody **IOD** wykorzystywanie urządzeń do niejawnego przekazywania lub rejestracji danych dotyczących informacji chronionych, w tym głosu i obrazu, tj.: magnetofonów, dyktafonów, aparatów fotograficznych, kamer, telefonów komórkowych z opcją rejestrowania dźwięku i obrazu, rejestratorów ruchu sieciowego, rejestratorów pracy klawiatur itp.
 7. Powyższy zakaz nie dotyczy sytuacji, gdy rejestrowane są dane pochodzące z systemu testowego, a działania pracownika nie prowadzą, i w sposób oczywisty nie mogą prowadzić, do odczytywania jakichkolwiek poufnych informacji, do których pracownik nie ma dostępu.
 8. Wykorzystanie należących do Administratora danych urządzeń, systemów i oprogramowania oraz innych zasobów do prywatnych celów pracowników jest dozwolone jedynie na uzasadniony wniosek pracownika i za zgodą IOD i ASI.
 9. Zasoby Administratora danych powinny być przechowywane w taki sposób, aby zapobiec możliwości ich kradzieży lub uszkodzenia przez osoby postronne oraz przypadkowe uszkodzenia przez osoby lub czynniki środowiskowe.
 10. Wynoszenie aktywów (zasobów i informacji) poza obszar przetwarzania danych możliwe jest za zgodą **IOD** lub **ADO**.
 11. Zakazane jest przysyłanie informacji podlegających ochronie na prywatne adresy poczty elektronicznej oraz prowadzenie korespondencji służbowej z wykorzystaniem prywatnego adresu e-mail użytkownika.
 12. Zakazane jest używanie prywatnych nośników zewnętrznych (np. typu pendrive) i tworzenie nieautoryzowanych kopii z baz danych.
 13. Pracownicy zobowiązani są stosować zasadę czystego biurka i ekranu - wszystkie dokumenty i materiały powinny być po zakończeniu pracy chowane w przeznaczonych do tego szafkach, szufladach itp. W przypadku braku dostatecznej ilości dostępnego miejsca dokumenty i materiały powinny być pozostawiane na biurku uporządkowane.
 14. Pracownicy są zobowiązani do ochrony zasobów będących własnością innych podmiotów, a powierzonych lub oddanych do dyspozycji Administratorowi danych lub udostępnionych pracownikom na czas wykonywania przez nich czynności służbowych w takim samym stopniu jak w przypadku zasobów będących własnością Administratora danych.
 15. Procedury i instrukcje dotyczące bezpieczeństwa teleinformatycznego opracowuje ASI i przechowuje w Teczce ODO.

§ 23

METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

1. Identyfikator

- 1) Identyfikator nadaje Administrator Sytemu Informatycznego lub Administrator Aplikacji.
- 2) Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.

2. Hasło użytkownika

- 1) Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem.
- 2) Użytkownicy powinni stosować hasła, które:
 - a) są łatwe do zapamiętania, a trudne do odgadnięcia,
 - b) nie są oparte na prostych skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących właściciela konta (np. imię, nazwisko, numer telefonu, data urodzenia itp.),
 - c) zawierają przynajmniej jedną dużą literę, jedną małą literę, jedną cyfrę lub znak specjalny.
- 3) Hasła powinny być często zmieniane, na przykład co 30 dni; **IOD** lub **ASI** może, w uzasadnionych sytuacjach polecić dokonanie zmiany hasła przez użytkownika np. po każdym incydencie lub podejrzeniu naruszenia bezpieczeństwa.
- 4) Należy unikać ponownego lub cyklicznego używania starych hasel.
- 5) Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych osobowych z identyfikatora lub hasła innego użytkownika.
- 6) Pracownicy są odpowiedzialni za zachowanie w poufności swoich hasel.
- 7) Użytkownik nie powinien przechowywać hasel w widocznych miejscach, nie powinien umieszczać hasel w żadnych automatycznych procesach logowania (skryptach, makrach lub pod klawiszami funkcyjnymi).
- 8) Użytkownik wprowadza swoje hasło w sposób uniemożliwiający innym osobom jego poznanie.
- 9) W sytuacji, gdy zachodzi podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik natychmiast dokonuje zmiany hasła.
- 10) Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
- 11) Administrator Systemu Informatycznego oraz Specjalista ds. odo przeprowadzają okresowe sprawdzanie, usuwanie lub blokowanie zbędnych identyfikatorów użytkowników oraz kont w systemach za które są odpowiedzialni.

3. Hasło administratora systemu informatycznego

Hasła użytkowników uprzywilejowanych (tzn. użytkowników posiadających uprawnienia na poziomie administratorów systemów informatycznych) są zabezpieczone u Administratora danych na wypadek sytuacji awaryjnych, szczególnie w przypadku nieobecności administratora systemu.

X. POSTANOWIENIA KOŃCOWE

§ 24

1. Do stosowania zasad określonych przez dokumenty Polityki zobowiązani są wszyscy pracownicy w rozumieniu przepisów Kodeksu Pracy i inne osoby mające dostęp do informacji podlegającej ochronie.
2. Z treścią niniejszego dokumentu powinni zapoznać się wszyscy pracownicy i inne osoby mające dostęp do informacji przetwarzanej u **ADO**, przed przystąpieniem do przetwarzania danych.
3. Niniejszy dokument może być przedstawiany podmiotom i jednostkom współpracującym z którymi współpraca może skutkować możliwością dostępu do informacji chronionych.
4. Wobec osoby, która w przypadku naruszenia ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne lub porządkowe.
5. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym **IOD**.
6. W przypadku naruszenia postanowień **Polityki** pracownik, który dopuścił się takiego naruszenia lub przyczynił do niego (umyślnie lub nieumyślnie) może zostać ukarany zgodnie z obowiązującym regulaminem pracy, obowiązującymi przepisami prawa z zakresu ochrony danych osobowych, a w skrajnych przypadkach pociągnięty do odpowiedzialności karnej.
7. Umyślne lub nieumyślne naruszenie postanowień **Polityki** lub niestosowanie się do poleceń służbowych w tym zakresie może być potraktowane jako naruszenie obowiązków pracowniczych.

§ 25

1. Polityka jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym w żadnej formie.
2. Użytkownicy są zobowiązani zapoznać się z treścią **Polityki**
3. Użytkownik zobowiązany jest złożyć oświadczenie o tym, iż został zaznajomiony z przepisami i zasadami z zakresu ochrony danych osobowych, z niniejszą Polityką, a także zobowiązać się do ich przestrzegania.
4. Wzór oświadczenia potwierdzającego zaznajomienie użytkownika z przepisami w zakresie ochrony informacji oraz z dokumentacją obowiązującą u Administratora

Danych, a także o zobowiązaniu się do ich przestrzegania, stanowi załącznik nr 5 do niniejszej **Polityki**.

5. Oświadczenia przechowywane są w aktach osobowych.

§ 26

1. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie aktualnie obowiązujące przepisy prawa w zakresie ochrony danych osobowych, szczególnie **RODO**.
2. Użytkownicy zobowiązani są do bezwzględnego stosowania postanowień zawartych w niniejszej Polityce. W wypadku odrębnych od zawartych w niniejszej **Polityce** uregulowań występujących w innych procedurach obowiązujących u Administratora Danych, użytkownicy mają obowiązek stosowania unormowań dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.



WÓJT
Włodzimierz Fraszczyk

XI. SPIS ZAŁĄCZNIKÓW

1. Wyznaczenie i obowiązki **IOD** - załącznik nr 1
2. Wyznaczenie Administratora Systemu Informatycznego - załącznik nr 2
3. Obszar przetwarzania danych - środki bezpieczeństwa - załącznik nr 3
4. Rejestr czynności przetwarzania - załącznik nr 4
5. Oświadczenie Użytkownika - załącznik nr 5
6. Upoważnienie do przetwarzania danych osobowych - załącznik nr 6
7. Plan audytu i przeglądów **Polityki** ochrony danych osobowych - załącznik nr 7
8. Procedura zarządzania ryzykiem - załącznik nr 8
9. Procedura zgłaszania naruszeń - załącznik nr 9
10. Polityka realizacji praw osób, których dane dotyczą, sposoby informowania i komunikacji oraz tryb wykonywania praw przez osobę, której dane dotyczą - załącznik nr 10
11. Polityka korzystania z usług podmiotów przetwarzających - załącznik nr 11
12. Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych zawierająca: Zasady użytkowania zasobów komputerowych i sieci komunikacyjnych - załącznik nr 12; Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osób odpowiedzialnych za te czynności - załącznik nr 15
13. Ewidencja osób upoważnionych - wzór - załącznik nr 13
14. Regulamin **IOD** - załącznik nr 14

Wypełnione załączniki przechowywane są w Teczce Ochrony Danych Osobowych.



WÓJT
Włodzimierz Fraszczyk

